(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－201169
（P2000－201169A）
(43)公開日　平成12年７月18日(2000.7.18)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｈ０４Ｌ	12/54		Ｈ０４Ｌ	11/20	１０１Ｂ　５Ｂ０８９
	12/58		Ｇ０６Ｆ	13/00	３５１Ｃ　５Ｊ１０４
Ｇ０６Ｆ	13/00	３５１	Ｇ０９Ｃ	1/00	６４０Ｂ　５Ｋ０３０
Ｇ０９Ｃ	1/00	６４０	Ｈ０４Ｌ	9/00	６７５Ｄ　９Ａ００１
Ｈ０４Ｌ	9/32				６７５Ｂ

審査請求　有　請求項の数112　ＯＬ　（全 65 頁）

(21)出願番号　特願平11－82211

(22)出願日　平成11年３月25日(1999.3.25)

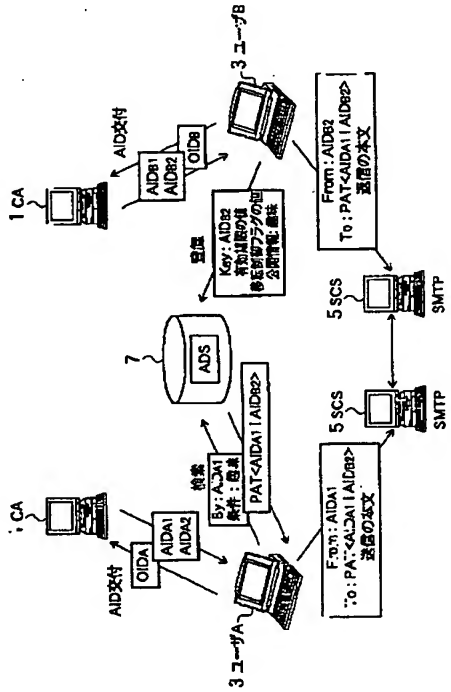
(31)優先権主張番号　特願平10－79837
(32)優先日　平成10年３月26日(1998.3.26)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平10－171930
(32)優先日　平成10年６月18日(1998.6.18)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平10－224861
(32)優先日　平成10年８月７日(1998.8.7)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　久田　裕介
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　小野　諭
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　メールアクセス制御方法、通信システム、およびメールアクセス制御プログラムを格納した記憶媒体

(57)【要約】
【課題】　匿名性とセキュリティを確保すべく発信者および着信者の匿名性を保持しつつ発信者からの通信の接続を可能とするメールアクセス制御方式を提供すること。
【解決手段】　着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取り、該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御する。また、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義し、通信ネットワーク上のメールの通信において各ユーザを各ユーザの役割識別子により識別する。



【特許請求の範囲】

【請求項１】　着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、
該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップと、
を有することを特徴とするメールアクセス制御方法。

【請求項２】　前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否することを特徴とする請求項１記載のメールアクセス制御方法。

【請求項３】　前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証することを特徴とする請求項２記載のメールアクセス制御方法。

【請求項４】　前記受け取るステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、前記制御するステップにおいて、該セキュア・コミュニケーション・サービスは発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否することを特徴とする請求項１記載のメールアクセス制御方法。

【請求項５】　前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否することを特徴とする請求項１記載のメールアクセス制御方法。

【請求項６】　前記個別化アクセスチケットの有効期限は信頼できる第三者機関により設定されたものであることを特徴とする請求項５記載のメールアクセス制御方法。

【請求項７】　各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理するディレクトリ・サービスにおいて、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者に対して前記個別化アクセスチケットを発行するステップを、更に有することを特徴とする請求項１記載のメールアクセス制御方法。

【請求項８】　そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み、該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを、予め前記セキュア・コミュニケーション・サービスに登録するステップを更に有し、
前記制御するステップにおいて、該セキュア・コミュニケーション・サービスは発信者により提示された個別化アクセスチケットがそこに予め登録されたものであるときには前記メールの配送を拒否することを特徴とする請求項１記載のメールアクセス制御方法。

【請求項９】　前記登録するステップにおいて個別化アクセスチケットを登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービスにおいて登録された個別化アクセスチケットを削除するステップを、更に有することを特徴とする請求項８記載のメールアクセス制御方法。

【請求項１０】　前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービスにより発信者を認証すべきかどうか示す移転制御フラグも含み、前記制御するステップにおいて、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、該セキュア・コミュニケーション・サービスは発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否することを特徴とする請求項１記載のメールアクセス制御方法。

【請求項１１】　前記発信者識別子の認証は、発信者と前記セキュア・コミュニケーション・サービス間のチャレンジ／レスポンス認証により実現することを特徴とする請求項１０記載のメールアクセス制御方法。

【請求項１２】　前記個別化アクセスチケットの移転制御フラグは信頼できる第三者機関により設定されたものであることを特徴とする請求項１０記載のメールアクセス制御方法。

【請求項１３】　前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の実メールアドレスにより与えられることを特徴とする請求項１記載のメールアクセス制御方法。

【請求項１４】　前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子

により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであることを特徴とする請求項１記載のメールアクセス制御方法。

【請求項１５】　前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項１４記載のメールアクセス制御方法。

【請求項１６】　前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項１４記載のメールアクセス制御方法。

【請求項１７】　前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする請求項１４記載のメールアクセス制御方法。

【請求項１８】　それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられることを特徴とする請求項１記載のメールアクセス制御方法。

【請求項１９】　前記各役割識別子のリンク情報は、前記認証局により各役割識別子に一意に付与された識別子であることを特徴とする請求項１８記載のメールアクセス制御方法。

【請求項２０】　前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする請求項１８記載のメールアクセス制御方法。

【請求項２１】　前記個別化アクセスチケットは、一つの発信者識別子と一つの着信者識別子を１対１に対応付けて含むことを特徴とする請求項１記載のメールアクセス制御方法。

【請求項２２】　前記個別化アクセスチケットは、一つの発信者識別子と複数の着信者識別子を１対Ｎ（Ｎは１より大きい整数）に対応付けて含むことを特徴とする請求項１記載のメールアクセス制御方法。

【請求項２３】　前記一つの発信者識別子と複数の着信者識別子の内の一識別子は前記個別化アクセスチケットの所有者を特定する所有者識別子であり、前記一つの発信者識別子と複数の着信者識別子の内の他の識別子は該所有者が属するグループの会員を特定する会員識別子であることを特徴とする請求項２２記載のメールアクセス制御方法。

【請求項２４】　各ユーザの識別子と、各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnabler を認証局において各ユーザに発行して、該個別化アクセスチケットに含まれる所有者識別子と該所有者識別子に対応するEnabler の両方をセキュアな演算装置に対して提示したユーザによってのみ該セキュアな演算装置において該個別化アクセスチケットに対する所定の演算を行えるようにするステップを、更に有することを特徴とする請求項２３記載のメールアクセス制御方法。

【請求項２５】　前記認証局は、それがEnabler であることを示す情報と各ユーザの識別子の実体に対し、該認証局の秘密鍵で署名したものを各ユーザの識別子のEnablerとして発行することを特徴とする請求項２４記載のメールアクセス制御方法。

【請求項２６】　前記所定の演算は、個別化アクセスチケットの新規作成、複数個別化アクセスチケットのマージ、一個別化アクセスチケットの複数個別化アクセスチケットへの分割、個別化アクセスチケットの所有者変更、個別化アクセスチケットの有効期限の変更、個別化アクセスチケットの移転制御フラグの変更、を含むことを特徴とする請求項２４記載のメールアクセス制御方法。

【請求項２７】　すべてのユーザに既知である特殊な識別子と該特殊な識別子に対応する特殊なEnabler を定義して、前記個別化アクセスチケットの新規生成および前記個別化アクセスチケットの所有者変更を、前記個別化アクセスチケットの所有者が、該特殊な識別子および該特殊なEnabler を用いて会員識別子のEnabler を使わずに行えるようにすることを特徴とする請求項２６記載のメールアクセス制御方法。

【請求項２８】　前記特殊な識別子は、個別化アクセスチケットの所有者識別子としてのみ使用可能であるように定義されていることを特徴とする請求項２７記載のメールアクセス制御方法。

【請求項２９】　すべてのユーザに既知である特殊な識別子を定義して、該特殊な識別子を用いて個別化アクセスチケットに読取専用属性を設定できるようにすることを特徴とする請求項２６記載のメールアクセス制御方法。

【請求項３０】　前記制御するステップにおいて、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、前記セキュア・コミュニケーション・サービスは、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメー

ル転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すことを特徴とする請求項１記載のメールアクセス制御方法。

【請求項３１】　それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義し、

通信ネットワーク上のメールの通信において各ユーザを各ユーザの役割識別子により識別する、ことを特徴とするメールアクセス制御方法。

【請求項３２】　前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項３１記載のメールアクセス制御方法。

【請求項３３】　前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項３１記載のメールアクセス制御方法。

【請求項３４】　着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子と着信者の役割識別子を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、

該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップ、

を更に有することを特徴とする請求項３１記載のメールアクセス制御方法。

【請求項３５】　前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする請求項３３記載のメールアクセス制御方法。

【請求項３６】　前記定義するステップは、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報も定義し、各役割識別子は各役割識別子のリンク情報も含むことを特徴とする請求項３１記載のメールアクセス制御方法。

【請求項３７】　前記各役割識別子のリンク情報は、前記認証局により各役割識別子に一意に付与された識別子であることを特徴とする請求項３６記載のメールアクセス制御方法。

【請求項３８】　着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、

該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップ、

を更に有することを特徴とする請求項３６記載のメールアクセス制御方法。

【請求項３９】　前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする請求項３８記載のメールアクセス制御方法。

【請求項４０】　複数のユーザ端末が接続された通信網と、

着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、該通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービス装置と、

を有することを特徴とするメールアクセス制御を実現した通信システム。

【請求項４１】　前記セキュア・コミュニケーション・サービス装置は発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否することを特徴とする請求項４０記載の通信システム。

【請求項４２】　前記個別化アクセスチケットを自身の秘密鍵により署名して発行するセキュアな演算装置を更に有し、

前記セキュア・コミュニケーション・サービス装置は該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証することを特徴とする請求項４１記載の通信システム。

【請求項４３】　前記セキュア・コミュニケーション・サービス装置は発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれ

ていないときには、前記メールの配送を拒否することを特徴とする請求項４０記載の通信システム。

【請求項４４】　前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記セキュア・コミュニケーション・サービス装置は発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否することを特徴とする請求項４０記載の通信システム。

【請求項４５】　前記個別化アクセスチケットの有効期限を設定する信頼できる第三者機関を更に有することを特徴とする請求項４４記載の通信システム。

【請求項４６】　各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者に対して前記個別化アクセスチケットを発行するディレクトリ・サービス装置を更に有することを特徴とする請求項４０記載の通信システム。

【請求項４７】　前記セキュア・コミュニケーション・サービス装置は、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め登録し、発信者により提示された個別化アクセスチケットがそこに予め登録されたものであるときには前記メールの配送を拒否することを特徴とする請求項４０記載の通信システム。

【請求項４８】　前記セキュア・コミュニケーション・サービス装置は、前記個別化アクセスチケットを登録した前記特定の登録者からの要求により、そこに登録された個別化アクセスチケットを削除することを特徴とする請求項４７記載の通信システム。

【請求項４９】　前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービス装置により発信者を認証すべきかどうか示す移転制御フラグも含み、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、該セキュア・コミュニケーション・サービス装置は発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否することを特徴とする請求項４０記載の通信システム。

【請求項５０】　前記発信者識別子の認証は、発信者と前記セキュア・コミュニケーション・サービス装置間のチャレンジ／レスポンス認証により実現することを特徴とする請求項４９記載の通信システム。

【請求項５１】　前記個別化アクセスチケットの移転制御フラグを設定する信頼できる第三者機関を更に有することを特徴とする請求項４９記載の通信システム。

【請求項５２】　前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の実メールアドレスにより与えられることを特徴とする請求項４０記載の通信システム。

【請求項５３】　それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子を発行する認証局装置を更に有し、

前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられることを特徴とする請求項４０記載の通信システム。

【請求項５４】　前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする請求項５３記載の通信システム。

【請求項５５】　前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする請求項５３記載の通信システム。

【請求項５６】　前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする請求項５３記載の通信システム。

【請求項５７】　それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とを発行する認証局装置を更に有し、

前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられることを特徴とする請求項４０記載の通信システム。

【請求項５８】　前記各役割識別子のリンク情報は、前記認証局装置により各役割識別子に一意に付与された識別子であることを特徴とする請求項５７記載の通信システム。

【請求項５９】　前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする請求項５７記載の通信システム。

【請求項６０】　前記個別化アクセスチケットは、一つ

の発信者識別子と一つの着信者識別子を１対１に対応付けて含むことを特徴とする請求項４０記載の通信システム。

【請求項６１】　前記個別化アクセスチケットは、一つの発信者識別子と複数の着信者識別子を１対Ｎ（Ｎは１より大きい整数）に対応付けて含むことを特徴とする請求項４０記載の通信システム。

【請求項６２】　前記一つの発信者識別子と複数の着信者識別子の内の一識別子は前記個別化アクセスチケットの所有者を特定する所有者識別子であり、前記一つの発信者識別子と複数の着信者識別子の内の他の識別子は該所有者が属するグループの会員を特定する会員識別子であることを特徴とする請求項６１記載の通信システム。

【請求項６３】　各ユーザの識別子と、各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnabler を各ユーザに発行する認証局装置と、

該個別化アクセスチケットに含まれる所有者識別子と該所有者識別子に対応するEnabler の両方を提示したユーザによってのみ該個別化アクセスチケットに対する所定の演算を行うことを可能としたセキュアな演算装置と、を更に有することを特徴とする請求項６２記載の通信システム。

【請求項６４】　前記認証局装置は、それがEnabler であることを示す情報と各ユーザの識別子の実体に対し、該認証局の秘密鍵で署名したものを各ユーザの識別子のEnablerとして発行することを特徴とする請求項６３記載の通信システム。

【請求項６５】　前記所定の演算は、個別化アクセスチケットの新規作成、複数個別化アクセスチケットのマージ、一個別化アクセスチケットの複数個別化アクセスチケットへの分割、個別化アクセスチケットの所有者変更、個別化アクセスチケットの有効期限の変更、個別化アクセスチケットの移転制御フラグの変更、を含むことを特徴とする請求項６３記載の通信システム。

【請求項６６】　すべてのユーザに既知である特殊な識別子と該特殊な識別子に対応する特殊なEnabler を定義して、前記個別化アクセスチケットの新規生成および前記個別化アクセスチケットの所有者変更を、前記個別化アクセスチケットの所有者が、該特殊な識別子および該特殊なEnabler を用いて会員識別子のEnabler を使わずに行えるようにしたことを特徴とする請求項６５記載の通信システム。

【請求項６７】　前記特殊な識別子は、個別化アクセスチケットの所有者識別子としてのみ使用可能であるように定義されていることを特徴とする請求項６６記載の通信システム。

【請求項６８】　すべてのユーザに既知である特殊な識別子を定義して、該特殊な識別子を用いて個別化アクセスチケットに読取専用属性を設定できるようにしたことを特徴とする請求項６５記載の通信システム。

【請求項６９】　前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、前記セキュア・コミュニケーション・サービス装置は、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すことを特徴とする請求項４０記載の通信システム。

【請求項７０】　それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義する認証局装置と、

そこでのメールの通信において各ユーザが各ユーザの役割識別子により識別される通信網と、

を有することを特徴とするメールアクセス制御を実現した通信システム。

【請求項７１】　前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする請求項７０記載の通信システム。

【請求項７２】　前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする請求項７０記載の通信システム。

【請求項７３】　着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子と着信者の役割識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、前記通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービス装置を更に有することを特徴とする請求項７０記載の通信システム。

【請求項７４】　前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする請求項７３記載の通信システム。

【請求項７５】　前記認証局装置は、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報も定義し、各役割識別子は各役割識別子のリンク情報も含むことを特徴とする請求項７０記載の通信システム。

【請求項７６】　前記各役割識別子のリンク情報は、前

記認証局装置により各役割識別子に一意に付与された識別子であることを特徴とする請求項７５記載の通信システム。

【請求項７７】　着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、前記通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスを更に有することを特徴とする請求項７５記載の通信システム。

【請求項７８】　前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする請求項７７記載の通信システム。

【請求項７９】　コンピュータハードウェアと、
着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、発信者と着信者間の通信を接続するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、
を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュア・コミュニケーション・サービス装置。

【請求項８０】　前記コンピュータソフトウェアは、発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項７９記載のセキュア・コミュニケーション・サービス装置。

【請求項８１】　前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記コンピュータソフトウェアは、該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証するように前記コンピュータハードウェアを動作させることを特徴とする請求項８０記載のセキュア・コミュニケーション・サービス装置。

【請求項８２】　前記コンピュータソフトウェアは、発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項７９記載のセキュア・コミュニケーション・サービス装置。

【請求項８３】　前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記コンピュータソフトウェアは、発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項７９記載のセキュア・コミュニケーション・サービス装置。

【請求項８４】　前記コンピュータソフトウェアは、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め前記セキュア・コミュニケーション・サービスに登録し、発信者により提示された個別化アクセスチケットが前記セキュア・コミュニケーション・サービスに予め登録されたものであるときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項７９記載のセキュア・コミュニケーション・サービス装置。

【請求項８５】　前記コンピュータソフトウェアは、個別化アクセスチケットを登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービスにおいて登録された個別化アクセスチケットを削除するように前記コンピュータハードウェアを動作させることを特徴とする請求項８４記載のセキュア・コミュニケーション・サービス装置。

【請求項８６】　前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービスにより発信者を認証すべきかどうか示す移転制御フラグも含み、前記コンピュータソフトウェアは、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする請求項７９記載のセキュア・コミュニケーション・サービス装置。

【請求項８７】　前記コンピュータソフトウェアは、前記発信者識別子の認証を、発信者と前記セキュア・コミュニケーション・サービス間のチャレンジ／レスポンス

認証により実現するように前記コンピュータハードウェアを動作させることを特徴とする請求項８６記載のセキュア・コミュニケーション・サービス装置。

【請求項８８】　前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであって、前記コンピュータソフトウェアは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータハードウェアを動作させることを特徴とする請求項７９記載のセキュア・コミュニケーション・サービス装置。

【請求項８９】　それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられ、前記コンピュータソフトウェアは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータハードウェアを動作させることを特徴とする請求項７９記載のセキュア・コミュニケーション・サービス装置。

【請求項９０】　前記コンピュータソフトウェアは、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すように前記コンピュータハードウェアを動作させることを特徴とする請求項７９記載のセキュア・コミュニケーション・サービス装置。

【請求項９１】　コンピュータハードウェアと、
個別化アクセスチケットの要求をユーザから受け取り、発信者識別子と着信者識別子を対応付けて含み、自身の秘密鍵により署名された個別化アクセスチケットを発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、
を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置。

【請求項９２】　コンピュータハードウェアと、
各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者に対して、発信者から指定された検索条件に応じて、検索条件を満たした非個人的公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、
を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるディレクトリ・サービス装置。

【請求項９３】　コンピュータハードウェアと、
それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を、各ユーザに対して発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、
を有することを特徴とする、メールアクセス制御を実現した通信システムにおける認証局装置。

【請求項９４】　コンピュータハードウェアと、
各ユーザの識別子と、一般に一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの中で該各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnabler を各ユーザに対して発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、
を有することを特徴とする、メールアクセス制御を実現した通信システムにおける認証局装置。

【請求項９５】　コンピュータハードウェアと、
一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの要求をユーザから受け取り、該ユーザが該個別化アクセスチケットに含まれる所有者識別子と該ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示し該所有者識別子に対応するEnabler の両方を提示したときに該個別化アクセスチケットに対する所定の演算を行うように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、
を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置。

【請求項９６】　着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを

制御して、発信者と着信者間の通信を接続する、メールアクセス制御を実現した通信システムにおけるセキュア・コミュニケーション・サービス装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項９７】　前記プログラムは、発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項９６記載の記憶媒体。

【請求項９８】　前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記プログラムは、該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証するように前記コンピュータを動作させることを特徴とする請求項９７記載の記憶媒体。

【請求項９９】　前記プログラムは、発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項９６記載の記憶媒体。

【請求項１００】　前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記プログラムは、発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項９６記載の記憶媒体。

【請求項１０１】　前記プログラムは、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め前記セキュア・コミュニケーション・サービス装置に登録し、発信者により提示された個別化アクセスチケットが前記セキュア・コミュニケーション・サービス装置に予め登録されたものであるときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項９６記載の記憶媒体。

【請求項１０２】　前記プログラムは、個別化アクセスチケットを登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービス装置において登録された個別化アクセスチケットを削除するように前記コンピュータを動作させることを特徴とする請求項１０１記載の記憶媒体。

【請求項１０３】　前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービス装置により発信者を認証すべきかどうか示す移転制御フラグも含み、前記プログラムは、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする請求項９６記載の記憶媒体。

【請求項１０４】　前記プログラムは、前記発信者識別子の認証を、発信者と前記セキュア・コミュニケーション・サービス装置間のチャレンジ／レスポンス認証により実現するように前記コンピュータを動作させることを特徴とする請求項１０３記載の記憶媒体。

【請求項１０５】　前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであって、前記プログラムは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータを動作させることを特徴とする請求項９６記載の記憶媒体。

【請求項１０６】　それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられ、前記プログラムは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータを動作させることを特徴とする請求項９６記載の記憶媒体。

【請求項１０７】　前記プログラムは、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すように前記コンピュータを動作させることを特徴とする請求項９６記載の記憶媒体。

【請求項１０８】　個別化アクセスチケットの要求をユ

ーザから受け取り、発信者識別子と着信者識別子を対応付けて含み、自身の秘密鍵により署名された個別化アクセスチケットを発行する、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項109】 各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者に対して、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを発行する、メールアクセス制御を実現した通信システムにおけるディレクトリ・サービス装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項110】 それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を、各ユーザに対して発行する、メールアクセス制御を実現した通信システムにおける認証局装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項111】 各ユーザの識別子と、一般に一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの中で各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnabler を各ユーザに対して発行する、メールアクセス制御を実現した通信システムにおける認証局装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【請求項112】 一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの要求をユーザから受け取り、該ユーザが該個別化アクセスチケットに含まれる所有者識別子と該ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示し該所有者識別子に対応するEnabler の両方を提示したときに該個別化アクセスチケットに対する所定の演算を行う、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置としてコンピュータを動作させるプログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信網において着信者の通信網における識別子を隠蔽しつつ、通信網における識別子を隠蔽した他のユーザからの通信の接続を制御してメールの送受信を制御するメールアクセス接続制御方法、通信システム、およびメールアクセス制御プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】インターネットの普及に伴い、メールを用いたＳＰＡＭや嫌がらせ行為が急増している。ＳＰＡＭとは受信者の時間的、経済的、精神的負担を考慮せず一方的に送り付けられるメールまたはニューズの総称である。メールによるＳＰＡＭはＵＢＥ(Unsolicited Bulk Email)またはＵＣＥ(Unsolicited Commercial Email)とも呼ばれている。

【0003】ＳＰＡＭは受信者の年齢、性別、嗜好等を考慮せず無差別に送信されるため、受信者にとって興味のない内容や不快な内容である場合が少なくない。受信に要する時間的負担や経済的負担も小さくない。ビジネスユーザにとっては、重要なメールがＳＰＡＭに埋もれて見つかりにくくなるため業務効率の低下を招きかねない。また、大量のユーザ宛に送信されるためネットワーク資源を浪費し、最悪の場合には過負荷を引き起こす。その結果、ユーザにとって重要なメールが失われる場合もある。また、匿名でまたは他人に成りすまして送信されるため、苦情対応のために人的資源を確保しなければならない。

【0004】一方、嫌がらせとは特定のユーザに対し精神的苦痛を与えたり、経済的、時間的負担を負わせるために、ユーザにとって不快な内容のメールを継続的に送り続ける行為である。ＳＰＡＭと同様に、実在または架空の第三者に成りすまして送信されるため、送信者の特定は極めて困難である。また、大容量メールを送り付けられたり、短時間に大量のメールを送り付けられたりするため、システムダウンの危険性もある。

【0005】ＳＰＡＭや嫌がらせ行為に対し、メールシステムは以下の要件を満足することが必要である。

【0006】・安全性

送信者の成りすましを検出し、配送を拒否することが必要である。

【0007】・堅牢性

大容量メールによるシステムダウンを回避するために、メール容量を制限することが必要である。また、大量送信によるシステムダウンを回避するために、送信回数を制限することが必要である。

【0008】・互換性

既存のメールシステムの実装を大きく変更しないことが必要である。

【0009】・操作性

既存のメールシステムの操作性を大きく変更しないことが必要である。

【0010】sendmail, qmail等のＭＴＡ(Message Transfer Agent)はエンベロープ情報及びヘッダ情報の偽造を検出し、配送を拒否する。また、MAPS RBL 等のいわゆるブラックリストを参照して、ＳＰＡＭの発信源となっているメールサーバからの受信を拒否する。また、PGP, S/MIME, TLS等を用いて署名確認を行うことにより他人の実メールアドレスを騙った送信を検出し、配送を拒

否する。また、本文の部分的削除によってメッセージ長を制限する。

【００１１】

【発明が解決しようとする課題】従来のメールシステムにおける実メールアドレスには以下のような問題点がある。

【００１２】・身元を推測可能

実メールアドレスは身元を推測する上で有益な情報を含むため、嫌がらせの相手を選択することができる。例えば、実ドメインから勤務先を特定できる。また、ユーザ名から性別や氏名を推測することができる。

【００１３】・身元から推測可能

実メールアドレスはユーザ名＠ドメイン名の形式で統一されているため、実メールアドレスを知らなくても、身元さえわかれば推測できる。例えば、氏名がわかればユーザ名の候補を絞り込むことができる。また、所属組織がわかればドメイン名の候補を絞り込むことができる。また、ユーザ名を実名とは無関係な文字列で与えている場合でも、ユーザ名の命名規則がわかれば試行錯誤的な送信によって推測できる。

【００１４】・移転可能

実メールアドレスは人から人に移転できるため、持ち主から直接教えてもらえなくても送信できる。メールを介した移転には以下の場合がある。他人の実メールアドレスをＣｃ：行に指定すれば、Ｔｏ：行に指定したすべての受信者に移転することができる。また、第三者の実メールアドレスをＲｅｐｌｙ－Ｔｏ：行に指定し、Ｔｏ：行に指定した受信者の実メールアドレスを本文に含むメールをフォワードすれば、その実メールアドレスを第三者に移転することができる。

【００１５】・取り消し困難

ＳＰＡＭや嫌がらせだけではなく重要なメールもよめなくなるため、実メールアドレスの取り消しは困難である。

【００１６】匿名リメーラ（anonymous remailers）と呼ばれるCypherpunk remailersとMixmaster remailersは送信者の実メールアドレス及び実ドメインを暗号化してから配送する。この方法はreply blockと呼ばれている。reply blockの暗号化及び復号化には匿名リメーラの公開鍵及び秘密鍵を用いるため、送信者以外のいかなるユーザも送信者の実メールアドレス及び実ドメインを特定することは困難である。

【００１７】匿名リメーラは実メールアドレスを特定困難なため、実メールアドレスの移転も困難である。しかしながら、reply blockは移転可能であるため、受信者以外のユーザからも送信者に対し返信することが可能である。

【００１８】偽名サーバ（pseudonymous server）と呼ばれるAS-Nodeとnym.alias.netはユーザの実メールアドレスと一意に対応した偽名アカウントを用いてメールを送受信する。偽名アカウントはユーザ側で任意に作成できるため、ユーザは実メールアドレスを推測困難な偽名アカウントを持つことが可能である。さらに、replyblockの利用により、ユーザの実メールアドレス及び実ドメインを偽名サーバに対し隠蔽することも可能である。これらの手段を組み合わせることによって、送信者以外のいかなるユーザも送信者の実メールアドレス及び実ドメインを特定することは困難となる。また、偽名アカウントは取り消し可能なため、実メールアドレスを取り消す必要もない。

【００１９】偽名サーバは実メールアドレスを特定困難なため、実メールアドレスの移転も困難である。しかしながら、偽名アカウントは移転可能なため、受信者以外のユーザからも送信することが可能である。

【００２０】さらに、ＳＰＡＭや嫌がらせ行為から受信者を保護するためには、これらの行為を行う発信者からの接続要求を拒否することも必要である。このため、通信システムは発信者の身元を一意に特定可能であることも必要である。

【００２１】これらのことから、通信システムはユーザの実メールアドレスを隠蔽しつつ（すなわち、ユーザの匿名性を保証しつつ）、そのユーザの身元を一意に特定可能であることが求められるが、従来の通信システムにおいて、これらの両者を同時に実現することは困難であった。

【００２２】メールシステムにおいてユーザの身元を特定するためには、そのユーザの実メールアドレスが必要である。一方、匿名リメーラは、発信者の匿名性保証のために発信者の実メールアドレスを暗号化または削除してから配送する。

【００２３】この条件において発信者の身元を特定するためには、トラフィック解析によってメールの配送経路を追跡することが必要である。ところが、匿名リメーラはメールの配送を遅らせたり、配送順序を入れ替えたりする。また、Mixmaster remailersはメールを複数のブロックに分割してから配送する。このため、トラフィック解析による配送経路の追跡は困難であり、発信者の身元特定も困難である。

【００２４】偽名サーバもメールの配送において匿名リメーラを利用するため、発信者の匿名性は保証できるけれども発信者の身元を一意に特定することは困難である。

【００２５】一方、ドイツ電子署名法は、通信サービスで用いられるディジタル署名を生成するためのディジタル証明書に対し、実名に加えて偽名の記入も許可している。ディジタル証明書はユーザに対し一意に付与されるため、偽名を記載してもユーザの身元を一意に特定することが可能である。また、偽名の命名権はユーザ側にあるため、実名を推測困難な偽名を記載することが可能である。

【００２６】本発明は、上記に鑑みてなされたもので、その目的とするところは、ＳＰＡＭや嫌がらせの原因となる実メールアドレスの問題点を解決する通信網におけるメールアクセス制御方式を提供することにある。

【００２７】本発明の他の目的は、ユーザの識別子を隠蔽しつつ、ユーザの身元を一意に特定可能にするメールアクセス制御方式を提供することにある。

【００２８】

【課題を解決するための手段】本発明では、実メールアドレスの移転及び取り消しの問題を解決するために、個別化アクセスチケットを用いたメールアクセス制御方式を用いる。移転の問題を解決するためには、送信者の実メールアドレスと受信者の実メールアドレスの両者を含む個別化アクセスチケット（ＰＡＴ：Personalized Access Ticket）を用いて宛先を指定する。また、取り消しの問題を解決するために、信頼できる第三者機関においてＰＡＴに有効期限を設定する。そして、有効期限を過ぎたＰＡＴを提示した送信者からのメールの配送を拒否する。また、実メールアドレスを取り消す代わりにＰＡＴをセキュア・コミュニケーション・サービスで管理するセキュアな記憶装置に登録する。

【００２９】すなわち、本発明では送信者の実メールアドレスと受信者の実メールアドレスを対にした単位で接続を制御する。このため、実メールアドレスを移転されても、移転先のユーザによってＰＡＴを取得されない限り、移転先のユーザからのメールを受信しないで済む。

【００３０】また、本発明では有効期限を過ぎたＰＡＴ、または受信者によってデータベースに登録されたＰＡＴを提示した送信者からのメールの配送をしないため、実メールアドレスを取り消すことなく受信を拒否できる。

【００３１】また、本発明ではＰＡＴを前記記憶装置から削除することにより受信を再開するため、実メールアドレスを再取得することなく受信を再開できる。

【００３２】また、本発明ではメールの送信をサーバ側で拒否するため、ユーザ側での受信やダウンロードに要する時間的、経済的負担を軽減できる。

【００３３】さらに、本発明では、ユーザの匿名性を保証しつつ、ユーザの身元特定を可能にするために、個人識別子と役割識別子を用いたメールアクセス制御方式を用いる。

【００３４】本発明では、ユーザを一意に特定するために、個人情報に信頼できる第三者機関の秘密鍵で署名した証明書を付与する。この証明書を以下では個人識別子（ＯＩＤ：Official Identification）と呼ぶ。また、ユーザの匿名性を保証しつつ身元特定を可能とするために、通信網上のユーザ識別子として個人識別子の情報を断片的に含む証明書を付与する。この証明書を以下では役割識別子（ＡＩＤ：Anonymous Identification）と呼ぶ。

【００３５】また、本発明では、身元を特定するために、複数のＡＩＤの同一性を判定しながらＯＩＤを再構築する。ＡＩＤの移転および取り消しの問題を解決するために、ＡＩＤをＰＡＴに含め、セキュア・コミュニケーション・サービスＳＣＳにおいてＰＡＴを検証する。

【００３６】また、本発明では、身元を明らかにしないまま不特定多数からのアクセスを求めるユーザ側の需要に対して、ＡＩＤを不特定多数から検索可能なディレクトリで管理し、宛先としてＡＩＤを含むＰＡＴを出力する。

【００３７】これにより、本発明ではＡＩＤはＯＩＤを断片的にしか含まないため、メールの送受信において身元を隠蔽できる。また、ＡＩＤを不特定多数から閲覧可能なディレクトリサービスに登録しても、身元を不特定多数に対して隠蔽できる。

【００３８】また、本発明では複数のＡＩＤの同一性を判定しながらＯＩＤを再構築することにより、確率的に身元を特定できる。このため、身元を明らかにしないＳＰＡＭや嫌がらせ行為への対策を立てることが可能である。

【００３９】また、本発明では実メールアドレスの代わりにＡＩＤをディレクトリで管理し、宛先としてＡＩＤを含むＰＡＴを出力することにより、身元を明らかにしないまま不特定多数からのアクセスを受け付けることが可能である。

【００４０】より詳細には、本発明は、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップと、を有することを特徴とするメールアクセス制御方法を提供する。

【００４１】また、本発明では、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否することを特徴とする。

【００４２】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証することを特徴とする。

【００４３】また、本発明では、前記受け取るステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、前記制御するステップにおいて、該セキュア・コミュニケーション・サービスは発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否することを特徴とする。

【００４４】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記制御するステップにおいて、前記セキュア・コミュニケーション・サービスは発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否することを特徴とする。

【００４５】また、本発明では、前記個別化アクセスチケットの有効期限は信頼できる第三者機関により設定されたものであることを特徴とする。

【００４６】また、本発明では、各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理するディレクトリ・サービスにおいて、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者に対して前記個別化アクセスチケットを発行するステップを、更に有することを特徴とする。

【００４７】また、本発明では、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み、該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを、予め前記セキュア・コミュニケーション・サービスに登録するステップを更に有し、前記制御するステップにおいて、該セキュア・コミュニケーション・サービスは発信者により提示された個別化アクセスチケットがそこに予め登録されたものであるときには前記メールの配送を拒否することを特徴とする。

【００４８】また、本発明では、前記登録するステップにおいて個別化アクセスチケットを登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービスにおいて登録された個別化アクセスチケットを削除するステップを、更に有することを特徴とする。

【００４９】また、本発明では、前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービスにより発信者を認証すべきかどうか示す移転制御フラグも含み、前記制御するステップにおいて、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、該セキュア・コミュニケーション・サービスは発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否することを特徴とする。

【００５０】また、本発明では、前記発信者識別子の認証は、発信者と前記セキュア・コミュニケーション・サービス間のチャレンジ／レスポンス認証により実現することを特徴とする。

【００５１】また、本発明では、前記個別化アクセスチケットの移転制御フラグは信頼できる第三者機関により設定されたものであることを特徴とする。

【００５２】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の実メールアドレスにより与えられることを特徴とする。

【００５３】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであることを特徴とする。

【００５４】また、本発明では、前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【００５５】また、本発明では、前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【００５６】また、本発明では、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする。

【００５７】また、本発明では、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられることを特徴とする。

【００５８】また、本発明では、前記各役割識別子のリンク情報は、前記認証局により各役割識別子に一意に付与された識別子であることを特徴とする。

【００５９】また、本発明では、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする。

【００６０】また、本発明では、前記個別化アクセスチケットは、一つの発信者識別子と一つの着信者識別子を１対１に対応付けて含むことを特徴とする。

【００６１】また、本発明では、前記個別化アクセスチケットは、一つの発信者識別子と複数の着信者識別子を１対Ｎ（Ｎは１より大きい整数）に対応付けて含むことを特徴とする。

【００６２】また、本発明では、前記一つの発信者識別子と複数の着信者識別子の内の一識別子は前記個別化アクセスチケットの所有者を特定する所有者識別子であり、前記一つの発信者識別子と複数の着信者識別子の内の他の識別子は該所有者が属するグループの会員を特定する会員識別子であることを特徴とする。

【００６３】また、本発明では、各ユーザの識別子と、各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnabler を認証局において各ユーザに発行して、該個別化アクセスチケットに含まれる所有者識別子と該所有者識別子に対応するEnabler の両方をセキュアな演算装置に対して提示したユーザによってのみ該セキュアな演算装置において該個別化アクセスチケットに対する所定の演算を行えるようにするステップを、更に有することを特徴とする。

【００６４】また、本発明では、前記認証局は、それがEnabler であることを示す情報と各ユーザの識別子の実体に対し、該認証局の秘密鍵で署名したものを各ユーザの識別子のEnablerとして発行することを特徴とする。

【００６５】また、本発明では、前記所定の演算は、個別化アクセスチケットの新規作成、複数個別化アクセスチケットのマージ、一個別化アクセスチケットの複数個別化アクセスチケットへの分割、個別化アクセスチケットの所有者変更、個別化アクセスチケットの有効期限の変更、個別化アクセスチケットの移転制御フラグの変更、を含むことを特徴とする。

【００６６】また、本発明では、すべてのユーザに既知である特殊な識別子と該特殊な識別子に対応する特殊なEnabler を定義して、前記個別化アクセスチケットの新規生成および前記個別化アクセスチケットの所有者変更を、前記個別化アクセスチケットの所有者が、該特殊な識別子および該特殊なEnabler を用いて会員識別子のEnabler を使わずに行えるようにすることを特徴とする。

【００６７】また、本発明では、前記特殊な識別子は、個別化アクセスチケットの所有者識別子としてのみ使用可能であるように定義されていることを特徴とする。

【００６８】また、本発明では、すべてのユーザに既知である特殊な識別子を定義して、該特殊な識別子を用いて個別化アクセスチケットに読取専用属性を設定できるようにすることを特徴とする。

【００６９】また、本発明では、前記制御するステップにおいて、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、前記セキュア・コミュニケーション・サービスは、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すことを特徴とする。

【００７０】さらに、本発明は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義し、通信ネットワーク上のメールの通信において各ユーザを各ユーザの役割識別子により識別する、ことを特徴とするメールアクセス制御方法を提供する。

【００７１】また、本発明では、前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【００７２】また、本発明では、前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【００７３】また、本発明では、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子と着信者の役割識別子を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップ、を更に有することを特徴とする。

【００７４】また、本発明では、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする。

【００７５】また、本発明では、前記定義するステップは、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報も定義し、各役割識別子は各役割識

別子のリンク情報も含むことを特徴とする。

【００７６】また、本発明では、前記各役割識別子のリンク情報は、前記認証局により各役割識別子に一意に付与された識別子であることを特徴とする。

【００７７】また、本発明では、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報を対応付けて含んだ個別化アクセスチケットを、発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスにおいて受け取るステップと、該セキュア・コミュニケーション・サービスにおいて、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御するステップ、を更に有することを特徴とする。

【００７８】また、本発明では、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するステップを、更に有することを特徴とする。

【００７９】さらに、本発明は、複数のユーザ端末が接続された通信網と、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、該通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービス装置と、を有することを特徴とするメールアクセス制御を実現した通信システムを提供する。

【００８０】また、本発明では、前記セキュア・コミュニケーション・サービス装置は発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否することを特徴とする。

【００８１】また、本発明では、前記個別化アクセスチケットを自身の秘密鍵により署名して発行するセキュアな演算装置を更に有し、前記セキュア・コミュニケーション・サービス装置は該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証することを特徴とする。

【００８２】また、本発明では、前記セキュア・コミュニケーション・サービス装置は発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否することを特徴とする。

【００８３】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記セキュア・コミュニケーション・サービス装置は発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否することを特徴とする。

【００８４】また、本発明では、前記個別化アクセスチケットの有効期限を設定する信頼できる第三者機関を更に有することを特徴とする。

【００８５】また、本発明では、各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者に対して前記個別化アクセスチケットを発行するディレクトリ・サービス装置を更に有することを特徴とする。

【００８６】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み、該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを、予め登録し、発信者により提示された個別化アクセスチケットがそこに予め登録されたものであるときには前記メールの配送を拒否することを特徴とする。

【００８７】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記個別化アクセスチケットを登録した前記特定の登録者からの要求により、そこに登録された個別化アクセスチケットを削除することを特徴とする。

【００８８】また、本発明では、前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービス装置により発信者を認証すべきかどうか示す移転制御フラグも含み、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、該セキュア・コミュニケーション・サービス装置は発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否することを特徴とする。

【００８９】また、本発明では、前記発信者識別子の認証は、発信者と前記セキュア・コミュニケーション・サービス装置間のチャレンジ／レスポンス認証により実現することを特徴とする。

【００９０】また、本発明では、前記個別化アクセスチ

ケットの移転制御フラグを設定する信頼できる第三者機関を更に有することを特徴とする。

【００９１】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の実メールアドレスにより与えられることを特徴とする。

【００９２】また、本発明では、それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子を発行する認証局装置を更に有し、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられることを特徴とする。

【００９３】また、本発明では、前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする。

【００９４】また、本発明では、前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする。

【００９５】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする。

【００９６】また、本発明では、それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とを発行する認証局装置を更に有し、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられることを特徴とする。

【００９７】また、本発明では、前記各役割識別子のリンク情報は、前記認証局装置により各役割識別子に一意に付与された識別子であることを特徴とする。

【００９８】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする。

【００９９】また、本発明では、前記個別化アクセスチケットは、一つの発信者識別子と一つの着信者識別子を１対１に対応付けて含むことを特徴とする。

【０１００】また、本発明では、前記個別化アクセスチケットは、一つの発信者識別子と複数の着信者識別子を１対Ｎ（Ｎは１より大きい整数）に対応付けて含むことを特徴とする。

【０１０１】また、本発明では、前記一つの発信者識別子と複数の着信者識別子の内の一識別子は前記個別化アクセスチケットの所有者を特定する所有者識別子であり、前記一つの発信者識別子と複数の着信者識別子の内の他の識別子は該所有者が属するグループの会員を特定する会員識別子であることを特徴とする。

【０１０２】また、本発明では、各ユーザの識別子と、各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnabler を各ユーザに発行する認証局装置と、該個別化アクセスチケットに含まれる所有者識別子と該所有者識別子に対応するEnabler の両方を提示したユーザによってのみ該個別化アクセスチケットに対する所定の演算を行うことを可能としたセキュアな演算装置と、を更に有することを特徴とする。

【０１０３】また、本発明では、前記認証局装置は、それがEnabler であることを示す情報と各ユーザの識別子の実体に対し、該認証局の秘密鍵で署名したものを各ユーザの識別子のEnablerとして発行することを特徴とする。

【０１０４】また、本発明では、前記所定の演算は、個別化アクセスチケットの新規作成、複数個別化アクセスチケットのマージ、一個別化アクセスチケットの複数個別化アクセスチケットへの分割、個別化アクセスチケットの所有者変更、個別化アクセスチケットの有効期限の変更、個別化アクセスチケットの移転制御フラグの変更、を含むことを特徴とする。

【０１０５】また、本発明では、すべてのユーザに既知である特殊な識別子と該特殊な識別子に対応する特殊なEnabler を定義して、前記個別化アクセスチケットの新規生成および前記個別化アクセスチケットの所有者変更を、前記個別化アクセスチケットの所有者が、該特殊な識別子および該特殊なEnabler を用いて会員識別子のEnabler を使わずに行えるようにしたことを特徴とする。

【０１０６】また、本発明では、前記特殊な識別子は、個別化アクセスチケットの所有者識別子としてのみ使用可能であるように定義されていることを特徴とする。

【０１０７】また、本発明では、すべてのユーザに既知である特殊な識別子を定義して、該特殊な識別子を用いて個別化アクセスチケットに読取専用属性を設定できるようにしたことを特徴とする。

【０１０８】また、本発明では、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、前記セキュア・コミュニケーション・サービス装置は、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メ

ールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すことを特徴とする。

【0109】さらに、本発明は、それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を定義する認証局装置と、そこでのメールの通信において各ユーザが各ユーザの役割識別子により識別される通信網と、を有することを特徴とするメールアクセス制御を実現した通信システムを提供する。

【0110】また、本発明では、前記各ユーザの役割識別子は、前記各ユーザの個人識別子の少なくとも一つの断片を含んだ情報に対し、前記認証局装置が該認証局装置の秘密鍵により署名したものであることを特徴とする。

【0111】また、本発明では、前記各ユーザの個人識別子は、前記認証局により各ユーザに一意に付与された文字列と各ユーザの公開鍵に対し、前記認証局が該認証局の秘密鍵により署名したものであることを特徴とする。

【0112】また、本発明では、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子と着信者の役割識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、前記通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービス装置を更に有することを特徴とする。

【0113】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする。

【0114】また、本発明では、前記認証局装置は、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報も定義し、各役割識別子は各役割識別子のリンク情報も含むことを特徴とする。

【0115】また、本発明では、前記各役割識別子のリンク情報は、前記認証局装置により各役割識別子に一意に付与された識別子であることを特徴とする。

【0116】また、本発明では、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、前記通信網上で発信者と着信者間の通信を接続するセキュア・コミュニケーション・サービスを更に有することを特徴とする。

【0117】また、本発明では、前記セキュア・コミュニケーション・サービス装置は、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定することを特徴とする。

【0118】さらに、本発明は、コンピュータハードウェアと、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、発信者と着信者間の通信を接続するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュア・コミュニケーション・サービス装置を提供する。

【0119】また、本発明では、前記コンピュータソフトウェアは、発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【0120】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記コンピュータソフトウェアは、該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証するように前記コンピュータハードウェアを動作させることを特徴とする。

【0121】また、本発明では、前記コンピュータソフトウェアは、発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【0122】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記コンピュータソフトウェア

は、発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【０１２３】また、本発明では、前記コンピュータソフトウェアは、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め前記セキュア・コミュニケーション・サービスに登録し、発信者により提示された個別化アクセスチケットが前記セキュア・コミュニケーション・サービスに予め登録されたものであるときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【０１２４】また、本発明では、前記コンピュータソフトウェアは、個別化アクセスチケットを登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービスにおいて登録された個別化アクセスチケットを削除するように前記コンピュータハードウェアを動作させることを特徴とする。

【０１２５】また、本発明では、前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービスにより発信者を認証すべきかどうか示す移転制御フラグも含み、前記コンピュータソフトウェアは、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否するように前記コンピュータハードウェアを動作させることを特徴とする。

【０１２６】また、本発明では、前記コンピュータソフトウェアは、前記発信者識別子の認証を、発信者と前記セキュア・コミュニケーション・サービス間のチャレンジ／レスポンス認証により実現するように前記コンピュータハードウェアを動作させることを特徴とする。

【０１２７】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであって、前記コンピュータソフトウェアは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータハードウェアを動作させることを特徴とする。

【０１２８】また、本発明では、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられ、前記コンピュータソフトウェアは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータハードウェアを動作させることを特徴とする。

【０１２９】また、本発明では、前記コンピュータソフトウェアは、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すように前記コンピュータハードウェアを動作させることを特徴とする。

【０１３０】さらに、本発明は、コンピュータハードウェアと、個別化アクセスチケットの要求をユーザから受け取り、発信者識別子と着信者識別子を対応付けて含み、自身の秘密鍵により署名された個別化アクセスチケットを発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置を提供する。

【０１３１】さらに、本発明は、コンピュータハードウェアと、各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者に対して、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるディレクトリ・サービス装置を提供する。

【０１３２】さらに、本発明は、コンピュータハードウェアと、それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を、各ユーザに対して発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システ

ムにおける認証局装置を提供する。

【０１３３】さらに、本発明は、コンピュータハードウェアと、各ユーザの識別子と、一般に一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの中で該各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnabler を各ユーザに対して発行するように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおける認証局装置を提供する。

【０１３４】さらに、本発明は、コンピュータハードウェアと、一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの要求をユーザから受け取り、該ユーザが該個別化アクセスチケットに含まれる所有者識別子と該ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示し該所有者識別子に対応するEnabler の両方を提示したときに該個別化アクセスチケットに対する所定の演算を行うように前記コンピュータハードウェアを動作させるコンピュータソフトウェアと、を有することを特徴とする、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置を提供する。

【０１３５】さらに、本発明は、着信者にメールの送信を希望する発信者により着信者をメールの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを受け取り、該個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権を検証することにより発信者と着信者間のアクセスを制御して、発信者と着信者間の通信を接続する、メールアクセス制御を実現した通信システムにおけるセキュア・コミュニケーション・サービス装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【０１３６】また、本発明では、前記プログラムは、発信者により提示された前記個別化アクセスチケットを認証し、発信者により提示された該個別化アクセスチケットが改竄されているときには、前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【０１３７】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットを発行したセキュアな演算装置の秘密鍵により署名されており、前記プログラムは、該セキュアな演算装置の公開鍵により該個別化アクセスチケット内の該セキュアな演算装置の署名を検証することにより、該個別化アクセスチケットを認証するように前記コンピュータを動作させることを特徴とする。

【０１３８】また、本発明では、前記プログラムは、発信者により前記個別化アクセスチケットと共に提示された発信者識別子も受け取り、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれているか否かチェックし、発信者により提示された該発信者識別子が発信者により提示された該個別化アクセスチケットに含まれていないときには、前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【０１３９】また、本発明では、前記個別化アクセスチケットは、該個別化アクセスチケットが有効である期間を示す有効期限も含み、前記プログラムは、発信者により提示された該個別化アクセスチケットに含まれた有効期限をチェックし、発信者により提示された該個別化アクセスチケットが既に切れた有効期限を含んでいるときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【０１４０】また、本発明では、前記プログラムは、そのユーザからの特定の登録者へのメールの配送が拒否されるべき特定のユーザの識別子を発信者識別子として含み該特定の登録者の識別子を着信者識別子として含んだ個別化アクセスチケットを予め前記セキュア・コミュニケーション・サービス装置に登録し、発信者により提示された個別化アクセスチケットが前記セキュア・コミュニケーション・サービス装置に予め登録されたものであるときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【０１４１】また、本発明では、前記プログラムは、個別化アクセスチケットを登録した前記特定の登録者からの要求により、前記セキュア・コミュニケーション・サービス装置において登録された個別化アクセスチケットを削除するように前記コンピュータを動作させることを特徴とする。

【０１４２】また、本発明では、前記個別化アクセスチケットは、前記セキュア・コミュニケーション・サービス装置により発信者を認証すべきかどうか示す移転制御フラグも含み、前記プログラムは、該個別化アクセスチケットに含まれる移転制御フラグが発信者を認証すべきであることを示すときに、発信者により提示された発信者識別子を認証し、該発信者識別子の認証が失敗したときには前記メールの配送を拒否するように前記コンピュータを動作させることを特徴とする。

【０１４３】また、本発明では、前記プログラムは、前記発信者識別子の認証を、発信者と前記セキュア・コミュニケーション・サービス装置間のチャレンジ／レスポンス認証により実現するように前記コンピュータを動作させることを特徴とする。

【０１４４】また、本発明では、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者と着信者の役割識別子により与えられ、各ユーザの役割識別子

は、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだものであって、前記プログラムは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれた該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータを動作させることを特徴とする。

【０１４５】また、本発明では、それにより認証局が各ユーザを一意に識別可能な各ユーザの個人識別子の断片を少なくとも一つ含んだ各ユーザの役割識別子と、それにより各役割識別子を一意に識別可能な各役割識別子のリンク情報とが定義され、前記個別化アクセスチケット内の発信者識別子と着信者識別子は発信者の役割識別子のリンク情報と着信者の役割識別子のリンク情報により与えられ、前記プログラムは更に、前記発信者により使われた複数の個別化アクセスチケットに含まれたリンク情報に対応する該発信者の複数の役割識別子の同一性を判定して、該発信者の個人識別子を再構成することにより、該発信者の身元を確率的に特定するように前記コンピュータを動作させることを特徴とする。

【０１４６】また、本発明では、前記プログラムは、前記個別化アクセスチケットに基づいて発信者の着信者に対するアクセス権が検証された場合には、発信者により提示された発信者識別子を用いて該個別化アクセスチケットから着信者識別子を取り出し、取り出した着信者識別子を用いて前記メールを実際にメールの配送処理を行うメール転送機能が解釈可能な形式に変換し、変換後の前記メールに該個別化アクセスチケットを添付して該メール転送機能に渡すように前記コンピュータを動作させることを特徴とする。

【０１４７】さらに、本発明は、個別化アクセスチケットの要求をユーザから受け取り、発信者識別子と着信者識別子を対応付けて含み、自身の秘密鍵により署名された個別化アクセスチケットを発行する、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【０１４８】さらに、本発明は、各登録者の識別子と、個人情報に比べて秘密性の低い公開情報を不特定多数から検索可能な状態で管理し、発信者に対して、発信者から指定された検索条件に応じて、検索条件を満たした公開情報の登録者の識別子を着信者識別子とし、検索条件と共に発信者により指定された発信者識別子を用いて、発信者識別子と着信者識別子を対応付けて含んだ個別化アクセスチケットを発行する、メールアクセス制御を実現した通信システムにおけるディレクトリ・サービス装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【０１４９】さらに、本発明は、それにより自身が各ユーザを一意に識別可能な各ユーザの個人識別子と、該各ユーザの個人識別子の断片を少なくとも一つ含んだ役割識別子を、各ユーザに対して発行する、メールアクセス制御を実現した通信システムにおける認証局装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【０１５０】さらに、本発明は、各ユーザの識別子と、一般に一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの中で各ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示す各ユーザの識別子のEnabler を各ユーザに対して発行する、メールアクセス制御を実現した通信システムにおける認証局装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【０１５１】さらに、本発明は、一つの発信者識別子と複数の着信者識別子を対応付けて含みそれらの内の一識別子が所有者識別子である個別化アクセスチケットの要求をユーザから受け取り、該ユーザが該個別化アクセスチケットに含まれる所有者識別子と該ユーザの識別子を所有者識別子として含む個別化アクセスチケットの変更権を示し該所有者識別子に対応するEnabler の両方を提示したときに該個別化アクセスチケットに対する所定の演算を行う、メールアクセス制御を実現した通信システムにおけるセキュアな演算装置としてコンピュータを動作させるプログラムを格納した記憶媒体を提供する。

【０１５２】

【発明の実施の形態】まず、図１乃至図７を参照して本発明の第１の実施形態について説明する。本発明のメールアクセス制御方法は、通信網における発信者および着信者の匿名性を保持しつつ、発信者と着信者間の双方向通信をも適宜可能とするものであり、基本的には着信者の本当の識別子を隠蔽した状態で、着信者の特性を表す情報のみを公開し、この公開された情報に基づいて、匿名性を保持したまま通信を希望する者に対して限定的なアクセス権を付与することにある。

【０１５３】具体的には、ユーザに対して個人情報を隠蔽した役割識別子（Anonymous Identification：ＡＩＤと略称する）を付与し、この役割識別子ＡＩＤをユーザの特性を表す情報である趣味、年齢、職業等のようなユーザをネットワーク上で特定はできないが、発信者にとって当該ユーザと通信する価値があるかどうかを判断するための有用な情報と組にしてネットワークに公開する。

【０１５４】また、発信者は、前記公開された情報を閲覧または検索することにより自分が通信したい相手を捜すことができる。すなわち、発信者が発信者自身の匿名性を保持したままある相手と通信したい場合には、その相手の役割識別子を指定し、個別化アクセスチケットＰＡＴ（Personalized Access Ticket）を取得する。

【0155】個別化アクセスチケットPATには、発信者、着信者それぞれの役割識別子AIDの他に、移転制御フラグ、および、有効期限の各情報が記載されている。移転制御フラグは、セキュア・コミュニケーション・サービスSCS（Secure Communication Service）が送信者に対し認証を実行するか否かを決定するために使用される。すなわち、移転制御フラグを立てると、SCSは、接続要求の際に、発信者に対し、例えば署名の検証等の認証を行う。また、移転制御フラグを立てない場合には、セキュア・コミュニケーション・サービスSCSは認証無しで接続要求をセキュア・コミュニケーション・サービスSCSが接続している物理的通信網に渡す。すなわち、移転制御は役割識別子AIDがこれを認証局CA(Certification Authority）から割り当てられたユーザによって正当に利用されているかを認証するために用いられる。

【0156】本発明のメールアクセス制御方法を実施する通信網においては、ユーザに対する役割識別子AIDの付与、役割識別子AIDと組み合わされた公開情報の保持、個別化アクセスチケットPATの発行、および個別化アクセスチケットPATに基づくメールアクセス制御はそれぞれ別の機関で行われている。これは、それぞれの行為に関して保持すべきセキュリティレベルに差があるので、別々の機関で実行した方がネットワーク全体のセキュリティの保持には好都合だからである。但し、公開情報の保持とPATの発行は同一の機関で行ってもよい。

【0157】図1は、本第1の実施形態の通信システムの全体構成図である。本実施形態はインターネットまたはイントラネット上の電子メールサービスを対象としたものである。図1において、1は認証局CAであり、個人識別子OIDの認証権限と役割識別子AIDの発行権限を有し、個人識別子OIDから役割識別子AIDを生成し、ユーザに対して役割識別子AIDを割り当てる機能を有する。3はユーザである。5はセキュア・コミュニケーション・サービスSCSであり、ユーザ3からの電子メールによる接続要求に対し接続を許可するか否かを、ユーザ3から提示された個別化アクセスチケットを用いて判定する。また、ユーザ3からの要求に基づいて、電子メールによる接続要求を拒否する。また、ユーザ3からの要求に基づいて、個人識別子OIDの同一性を判定する。7はアノニマス・ディレクトリ・サービスADSであり、役割識別子AID、移転制御フラグの値、有効期限の値、及び、ユーザ3についての公開情報（趣味等、氏名、電話番号、実Eメールアドレス等の個人情報に比べ秘密性の低いと考えられる情報）を管理するデータベースである。アノニマス・ディレクトリ・サービスADS7は、検索条件を提示したユーザ3の役割識別子AID、検索条件を満足する公開情報をアノニマス・ディレクトリ・サービスADS7に登録していたユーザ3の役割識別子AID、ユーザ3または管理者等により与えられた移転制御フラグの値、及び、ユーザ3または管理者等により与えられた有効期限の値から個別化アクセスチケットPATを生成し、検索条件を提示したユーザ3に割り当てる機能を有する。

【0158】まず、ユーザの要求に基づいて個人識別子から役割識別子AIDを生成し、そのユーザに割り当てるまでの一連の処理について説明する。

【0159】図2は、個人識別子OID、役割識別子AIDおよび個別化アクセスチケットPATの例を示している。個人識別子OIDは、図2（a）に示すように、認証局CA1がユーザを一意に識別可能な規則に従う任意の文字列と公開鍵から構成される情報に対し、認証局CA1が署名したものである。また、役割識別子AIDは、図2（b）に示すように、個人識別子OIDの断片とその位置情報、冗長な文字列、SCSを動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列（ホスト名、実ドメイン名等）であるSCSの情報から構成される情報に対し、認証局CA1が署名したものである。

【0160】また、個別化アクセスチケットPATは、図2（c）に示すように、移転制御フラグ、役割識別子AID_0、役割識別子AID_1、有効期限から構成される情報に対して、アノニマス・ディレクトリ・サービスADSが署名したものである。ここで、移転制御フラグの値は、0または1のいずれかであると定義する。また、有効期限はPATの使用回数、PATが利用不可能になる絶対時刻（UTC）、PATが利用可能になる絶対時刻（UTC）、PATが利用可能になってから利用不可能になるまでの相対時間（寿命）のいずれか、または複数を組み合わせて定義する。

【0161】更に、後述する各実施形態で説明するように、本発明は、個別化アクセスチケットPATとして、上述した1対1個別化アクセスチケットに加えて、発信者と着信者を1対Nに対応させている1対N個別化アクセスチケット、および役割識別子の実体を個別化アクセスチケットで指定する代わりに役割識別子を指定するリンク情報を持ち、このリンク情報で役割識別子を指定するリンク指定型個別化アクセスチケットを有し、このリンク指定型個別化アクセスチケットには上述した発信者と着信者の対応関係に基づきリンク指定型1対1個別化アクセスチケットとリンク指定型1対N個別化アクセスチケットがある。すなわち、本発明の個別化アクセスチケットには、1対1個別化アクセスチケット、1対N個別化アクセスチケット、リンク指定型1対1個別化アクセスチケット、およびリンク指定型1対N個別化アクセスチケットの4種類がある。

【0162】次に、ユーザ3が役割識別子AIDを認証局CA1に対して要求する手続きについて説明する。ユーザ3は秘密鍵と公開鍵のペアを生成する。次に、ユー

ザ３の個人識別子ＯＩＤと認証局ＣＡ１の証明書を用いて、ユーザ３と認証局ＣＡ１との間で双方向認証を行う。次に、ユーザ３は該公開鍵を認証局ＣＡ１に任意の手段で送信する。

【０１６３】なお、上記手続きにおいて、ユーザ３と認証局ＣＡ１間の通信を暗号化する場合もある。

【０１６４】次に、上述した役割識別子ＡＩＤの要求に対し、認証局ＣＡ１が役割識別子ＡＩＤをユーザ３に対して交付する手続きについて説明する。認証局ＣＡ１は、ユーザ３からの公開鍵を受信すると、役割識別子ＡＩＤを生成する。次に、認証局ＣＡ１は該役割識別子ＡＩＤをユーザ３に任意の手段で送信する。ユーザ３は認証局ＣＡ１から役割識別子ＡＩＤを受信すると、受信した該役割識別子をユーザ３の記憶装置に記録する。

【０１６５】なお、上記手続きにおいて、ユーザ３と認証局ＣＡ１間の通信を暗号化する場合もある。

【０１６６】次に、認証局ＣＡ１における役割識別子ＡＩＤの生成処理について図３に示すフローチャートを用いて説明する。図３において、認証局ＣＡ１は個人識別子ＯＩＤの全長Ｌと等しい長さの情報を生成する。この情報を仮の役割識別子ＡＩＤとする（ステップＳ９１１）。次に、ＯＩＤの部分複写を行うために、ＯＩＤの複写範囲を指定するパラメータp_iとl_iの値をそれぞれ乱数発生等の任意の手段を用いて決定する（ステップＳ９１３）。ここで、Ｌは個人識別子ＯＩＤの全長と等しく、l_iは$0 \leq p_i \leq L$の関係が成立する範囲で任意に定めた値とする。次に、ＯＩＤの先頭から位置p_Iから位置$p_i + l_i$の範囲の情報を、仮ＡＩＤの同じ位置に複写する（ステップＳ９１５）。つまり、このＯＩＤ断片は仮ＡＩＤの先頭から位置p_iと位置$p_i + l_i$の範囲に複写される。次に、ＯＩＤを部分複写した仮ＡＩＤの定められた範囲に、p_iとl_iの値を任意の手段で暗号化して書き込む（ステップＳ９１７）。次に、これらの値を書き込んだ仮ＡＩＤの定められた範囲にセキュア・コミュニケーション・サービスＳＣＳ５を動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列（ホスト名、実ドメイン等）であるＳＣＳの情報を書き込む（ステップＳ９１９）。次に、文字列を書き込んだ仮ＡＩＤに認証局ＣＡ１の秘密鍵で署名する（ステップＳ９２１）。

【０１６７】次に、ユーザＢ３の役割識別子ＡＩＤ及び公開情報をアノニマス・ディレクトリ・サービスＡＤＳ７に登録する手続きについて説明する。登録者であるユーザＢ３とアノニマス・ディレクトリ・サービスＡＤＳ７との間で、ユーザＢ３の役割識別子ＡＩＤとＡＤＳ７の証明書を用いて、任意の手段で双方向認証を行う。次に、ユーザＢ３は、移転制御フラグの値、有効期限の値、および、趣味等の公開情報をＡＤＳ７に送信する。次に、ＡＤＳ７はユーザＢ３から受信した移転制御フラグの値、有効期限の値、すべての公開情報を、すべてユーザＢ３のＡＩＤと関連付けて記憶装置に記録する。

【０１６８】なお、上記手続きにおいて、登録者であるユーザＢ３とＡＤＳ７間の通信を暗号化する場合もある。

【０１６９】次に、ユーザＡ３がアノニマス・ディレクトリ・サービスＡＤＳ７に登録された公開情報を検索する手続きについて説明する。検索者であるユーザＡ３とアノニマス・ディレクトリ・サービスＡＤＳ７との間で、ユーザＡ３の役割識別子ＡＩＤとＡＤＳ７の証明書を用いて、任意の手段で双方向認証を行う。次にユーザＡ３は任意の検索条件をＡＤＳ７に送信する。次に、ＡＤＳ７は受信したすべての検索条件を記憶装置に提示し、これらの検索条件を満足する登録者の役割識別子ＡＩＤを抽出する。次に、ＡＤＳ７はユーザＡ３のＡＩＤと検索条件を満足した登録者のＡＩＤと移転制御フラグの値と有効期限の値から個別化アクセスチケットＰＡＴを生成する。次に、ＡＤＳ７は生成したＰＡＴをユーザＡ３に送信する。

【０１７０】なお、上記手続きにおいて、検索者であるユーザＡ３とＡＤＳ７間の通信を暗号化する場合もある。

【０１７１】１対１個別化アクセスチケットは、アノニマス・ディレクトリ・サービスＡＤＳ７の検索結果として生成する。

【０１７２】次に、図４に示すフローチャートを参照して、ＡＤＳにおける１対１個別化アクセスチケットＰＡＴの生成処理について説明する。まず、ある定められた長さの情報を生成する。これを仮の個別化アクセスチケット（仮ＰＡＴ）とする（ステップＳ１２１０）。次に、検索者であるユーザＡ３の役割識別子ＡＩＤと登録者であるユーザＢ３の役割識別子ＡＩＤを仮ＰＡＴの定められた範囲に複写する）（ステップＳ１２１５）。次に、移転制御フラグの値と有効期限の値をそれぞれ、ＡＩＤを複写した仮ＰＡＴの定められた範囲に書き込む（ステップＳ１２１７）。次に、これらの値を書き込んだ仮ＰＡＴにＡＤＳの秘密鍵で署名する（ステップＳ１２１９）。

【０１７３】次に、１対１個別化アクセスチケットＰＡＴによる移転制御について説明する。移転制御とは、ＰＡＴを譲渡されたあるいは盗聴した第三者（本来はアクセス権を有していないユーザ）から、正当なアクセス権を持つユーザへのアクセスを制限する機能である。

【０１７４】アノニマス・ディレクトリ・サービスＡＤＳ７および登録者ＡＩＤのユーザＢ３は、個別化アクセスチケットＰＡＴの移転制御フラグにある値を設定することにより、アクセス権を有していない第三者からのユーザＢ３への接続を禁止することができる。

【０１７５】移転制御フラグの値を１に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５と発信者との間で任意のチャレンジ／レスポンス方式に

従い発信者役割識別子ＡＩＤを認証するため、発信者が発信者ＡＩＤとＰＡＴの両者を発信者以外のいかなるユーザに渡しても、そのユーザは登録者にＳＣＳ５を介して接続できない。

【０１７６】一方、移転制御フラグの値を０に設定した場合には、ＳＣＳ５と発信者との間でいかなるチャレンジ／レスポンスも行わないため、発信者が発信者ＡＩＤとＰＡＴの両者を発信者以外のユーザに渡したら、それらのユーザもアノニマス・ディレクトリ・サービスの登録者とＳＣＳ５を介して接続できるようになる。

【０１７７】次に、図５を参照してＳＣＳにおけるメールアクセス制御方法について説明する。

【０１７８】発信者はＦｒｏｍ：行に”発信者ＡＩＤ@発信者のＳＣＳの実ドメイン”、Ｔｏ：行に”ＰＡＴ@発信者のＳＣＳの実ドメイン”の形式で指定する。

【０１７９】ＳＣＳはＳＭＴＰ(Simple Mail Transfer Protocol)等のＭＴＡ(Message Transfer Agent)の受信したメールを取得し、図５に示す処理を実行する。

【０１８０】１．ＰＡＴの署名をＡＤＳ７の公開鍵を用いて検証する（ステップＳ１４１３）。

【０１８１】・ＰＡＴに改竄が認められる場合（ステップＳ１４１５ＹＥＳ）、メールを廃棄して終了する（ステップＳ１４１６）。

【０１８２】・ＰＡＴに改竄が認められ得ない場合（ステップＳ１４１５ＮＯ）、下記処理２．を実行する。

【０１８３】２．発信者ＡＩＤをＰＡＴに提示して検索する（ステップＳ１４１７、Ｓ１４１９、Ｓ１４２１）。

【０１８４】・発信者ＡＩＤと完全一致するＡＩＤがＰＡＴに含まれていない場合には（ステップＳ１４２３ＮＯ）、メールを廃棄して終了する（ステップＳ１４１６）。

【０１８５】・発信者ＡＩＤと完全一致するＡＩＤがＰＡＴに含まれている場合には（ステップＳ１４２３ＹＥＳ）、下記処理３．を実行する。

【０１８６】３．ＰＡＴの有効期限の値を評価する（ステップＳ１４２５、Ｓ１４２７）。

【０１８７】・ＰＡＴが有効期限外の場合には（ステップＳ１４２７ＮＯ）、メールを廃棄して終了する（ステップＳ１４１６）。

【０１８８】・ＰＡＴが有効期限内の場合には（ステップＳ１４２７ＹＥＳ）、下記処理４．を実行する。

【０１８９】４．ＰＡＴの移転制御フラグの値を参照して、発信者を認証するか否かを決定する（ステップＳ１４３１、Ｓ１４３３）。

【０１９０】・値が１の場合には（ステップＳ１４３３ＹＥＳ）、ＳＣＳと発信者との間でチャレンジ／レスポンス認証を実行し、発信者の署名を検証する(ステップＳ１４３５）。署名が正しい場合には、着信者を指定し、ＰＡＴを添付する（ステップＳ１４３７）。署名が正しくない場合には、メールを廃棄して終了する（ステップＳ１４１６）。

【０１９１】・値が０の場合には（ステップＳ１４３３ＮＯ）、チャレンジ／レスポンス認証を実行せずに、着信者を指定し、ＰＡＴを添付する（ステップＳ１４３７）。

【０１９２】次に、ＳＣＳと発信者との間のチャレンジ／レスポンスの例を説明する。まず、ＳＣＳは任意の情報、例えばタイムスタンプを生成し、生成した情報を発信者に送信する。

【０１９３】次に、発信者は、受信した情報に発信者ＡＩＤの秘密鍵で署名し、発信者ＡＩＤの公開鍵とあわせてＳＣＳに送信する。

【０１９４】ＳＣＳは、受信した情報の署名を発信者ＡＩＤの公開鍵を用いて検証する。署名が正しい場合には、着信者を指定し、ＰＡＴを添付する。署名が正しくない場合にはメールを廃棄して終了する。

【０１９５】次に、ＳＣＳにおける着信者の指定方法について説明する。ＳＣＳは、まず、発信者ＡＩＤをＰＡＴに提示して検索し、発信者ＡＩＤと完全一致しないすべてのＡＩＤを取得する。取得したすべてのＡＩＤを以後、着信者ＡＩＤと定義する。次に、すべての着信者ＡＩＤについて、それぞれ、着信者ＡＩＤから着信者のＳＣＳの実ドメインを取り出す。次に、着信者を”着信者ＡＩＤ@着信者のＳＣＳの実ドメイン”の形式で指定する。最後に、ＳＣＳは発信者を”発信者ＡＩＤ@発信者のＳＣＳの実ドメイン”の形式から”発信者ＡＩＤ”の形式に変更する。

【０１９６】次に、ＳＣＳにおけるＰＡＴの添付方法について説明する。ＳＣＳは、ＰＡＴをメールの任意の箇所に添付する。

【０１９７】発信者及び受信者を指定しＰＡＴを添付してから、ＳＣＳは、ＭＴＡにメールを渡す。

【０１９８】なお、上記すべての処理は、１対Ｎ個別化アクセスチケットの場合も同様である。

【０１９９】次に、ＳＣＳにおける個別化アクセスチケットＰＡＴに対する着信拒否方法について説明する。

【０２００】着信拒否の設定：ユーザとセキュア・コミュニケーション・サービスＳＣＳ５との間で、任意の手段で双方向認証を行う。次に、ユーザは登録命令とユーザ自身のＡＩＤと任意のＰＡＴをＳＣＳ５に送信する。次に、ＳＣＳ５は受信したＡＩＤの署名を検証する。署名が正しくない場合には、ＳＣＳ５は処理を終了する。署名が正しい場合には、ＳＣＳ５は受信したすべてのＰＡＴについて、それぞれＡＤＳの公開鍵を用いて署名を検証する。署名が正しくないＰＡＴについては廃棄する。署名が正しい場合には、受信したＡＩＤをそれぞれのＰＡＴに提示して検索する。受信したＡＩＤと完全一致するＡＩＤを含むＰＡＴについては、登録命令とＰＡＴを記憶装置に提示して、ＰＡＴを記憶装置に登録す

る。受信したＡＩＤと完全一致するＡＩＤを含まないＰＡＴについては記憶装置に登録せずに廃棄する。なお、上記処理において、ユーザとＳＣＳ５間の通信を暗号化する場合もある。

【０２０１】着信拒否の実行：ＳＣＳ５はＰＡＴを記憶装置に提示して検索する。提示したＰＡＴと完全一致するＰＡＴが記憶装置に登録されている場合には、メールを廃棄する。提示したＰＡＴと完全一致するＰＡＴが記憶装置に登録されていない場合には、メールを廃棄しない。

【０２０２】着信拒否の解除：ユーザとセキュア・コミュニケーション・サービスＳＣＳ５との間で、任意の手段で双方向認証を行う。次に、ユーザは自らのＡＩＤをＳＣＳ５に提示する。次に、ＳＣＳ５は受信したＡＩＤの署名を検証する。署名が正しくない場合には、ＳＣＳ５は処理を終了する。署名が正しい場合には、ＳＣＳ５は提示されたＡＩＤを検索条件として記憶装置に提示して、提示されたＡＩＤを含むすべてのＰＡＴを取得し、ユーザに提示する。次に、ユーザは提示されたすべてのＰＡＴを参照し、着信拒否を解除したいＰＡＴをすべて選択し、削除命令と併せてＳＣＳ５に送信する。削除命令と着信拒否を解除したいすべてのＰＡＴを受信したＳＣＳ５は、受信した削除命令及びすべてのＰＡＴを記憶装置に提示して、受信したすべてのＰＡＴを記憶装置から削除する。

【０２０３】なお、ＳＣＳにおける１対Ｎ個別化アクセスチケットＰＡＴに対する着信拒否方法も、上記１対１個別化アクセスチケットに対する着信拒否方法と同様である。

【０２０４】また、ユーザＢからユーザＡへのメールの返信は、ユーザＡからユーザＢへのメールの送信の場合と同様である。

【０２０５】次に、図６のフローチャート及び図７を参照して、同一性の判定について説明する。

【０２０６】１．変数OID_Mの初期値を、ＯＩＤの全長Ｌと等しい長さで、かつ、すべての値が０であるビット列と定義する。また、変数OID_Vの初期値を、ＯＩＤの全長Ｌと等しい長さで、かつ、すべての値が０であるビット列と定義する（ステップＳ２５１１）。

【０２０７】２．処理対象のＡＩＤの集合から１個のＡＩＤを選択し、以下のビット演算を実行する（ステップＳ２５１３）。

【０２０８】(a) ＡＩＤに含まれる位置情報をもとにして、変数AID_Mと変数AID_Vの値を決定する（ステップＳ２５１５）。ここで、

・AID_MはＯＩＤの全長Ｌと等しい長さで、かつ、
－ＯＩＤ情報が定義されている位置の値は１である。
－ＯＩＤ情報が定義されていない位置の値は０である。
ビット列と定義する(図７)。

・AID_VはＯＩＤの全長Ｌと等しい長さで、かつ、
－ＯＩＤ情報が定義されている位置の値はＯＩＤ情報の実際の値である。
－ＯＩＤ情報が定義されていない位置の値は０である。
ビット列と定義する（図７）。

【０２０９】(b) OID_MとAID_MのＡＮＤ演算を実行し、その結果を変数OVR_Mに代入する（ステップＳ２５１７）。

【０２１０】(c) OVR_MとAID_MのＡＮＤ演算と、OVR_MとOID_MのＡＮＤ演算を実行し、その演算結果を比較する（ステップＳ２５１９）。

【０２１１】・一致する場合OID_MとAID_MのＯＲ演算を実行し、実行結果をOID_Mに代入する（ステップＳ２５２１）。また、OID_VとAID_VのＯＲ演算を実行し、実行結果をOID_Mに代入する（ステップＳ２５２３）。

【０２１２】・一致しない場合、ステップＳ２５２５に進み、実行する。

【０２１３】(d) 処理対象のＡＩＤの集合から、次に処理するＡＩＤを抽出する。

【０２１４】・集合に少なくとも１個のＡＩＤが含まれている場合、ステップＳ２５１３－Ｓ２５２３を実行する。

【０２１５】・集合にＡＩＤが１個も含まれていない場合、ステップＳ２５２７に進む。

【０２１６】(e) OID_MおよびOID_Vの値を出力する（ステップＳ２５２７）。

【０２１７】最終的に得られたOID_Mの値は、処理対象のＡＩＤの集合から復元できたＯＩＤ情報のすべての位置を表している。また、最終的に得られたOID_Vの値は、処理対象のＡＩＤの集合から復元できたＯＩＤ情報のすべてを表している。つまり、OID_MとOID_Vの値を用いると、

(a) OID_Vの値を検索条件とすると、確率的にではあるがＯＩＤを求めることができる。

【０２１８】(b) 上記検索の精度を、ＯＩＤ全長Ｌとの比OID_M／Ｌで定量的に評価することができる。

【０２１９】上述したように、本実施形態では、ユーザ要求に基づいて、秘密性且つ信用性の高い第三者機関である認証局ＣＡ１において、氏名、電話番号、実Ｅメールアドレス等秘密性の高い個人情報を含む個人識別子ＯＩＤからこれらの個人情報を隠蔽した役割識別子ＡＩＤを生成し、ユーザに交付する。このＡＩＤを用いて通信網及び通信網上で提供される各種サービスにおいてユーザを識別することにより、ユーザの匿名性保証と本人保証の両立が可能になる。つまり、ユーザは実名や電話番号やＥメールアドレスを相手に教えなくても、お互いに通信できるようになるし、後述のようにアノニマス・ディレクトリ・サービスＡＤＳ７を介して不特定多数に公開情報を開示することもできる。

【０２２０】ユーザは、個人情報に比べ秘密性のより低

いと思われる情報すなわち公開情報をアノニマス・ディレクトリ・サービスＡＤＳ７に登録する。公開情報及び登録者ＡＩＤを検索する場合には、検索者は検索者の役割識別子ＡＩＤと任意の検索条件をＡＤＳ７に提示する。ＡＤＳ７はすべての検索条件を満足する登録者の役割識別子ＡＩＤを抽出し、次に、検索者ＡＩＤと検索条件を満足した登録者のＡＩＤと移転制御フラグの値と有効期限の値から個別化アクセスチケットＰＡＴを生成する。

【０２２１】この１対１個別化アクセスチケットＰＡＴには、図２（ｃ）に示すように移転制御フラグの値、有効期限の値が設定されるが、この有効期限を事前に設定することにより、発信者からの接続を制限することができる。

【０２２２】また、移転制御フラグの値により、アクセス権を有していない第三者からの接続を禁止することができる。すなわち、移転制御フラグの値を１に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５と発信者との間で任意のチャレンジ／レスポンス方式に従い発信者役割識別子ＡＩＤを認証するため、発信者が発信者ＡＩＤとＰＡＴの両者を発信者以外のいかなるユーザに渡しても、そのユーザはアノニマス・ディレクトリ・サービスＡＤＳ７への登録者にＳＣＳ５を介して接続できない。一方、移転制御フラグの値を０に設定した場合には、ＳＣＳ５と発信者との間でいかなるチャレンジ／レスポンスも行わないため、発信者が発信者ＡＩＤとＰＡＴの両者を発信者以外のユーザに渡したら、それらのユーザもＡＤＳ７への登録者にＳＣＳ５を介して接続できるようになる。

【０２２３】また、１対１個別化アクセスチケットＰＡＴで着信者を指定した呼を個別化アクセスチケットＰＡＴ内で定義した着信者役割識別子ＡＩＤまたは発信者役割識別子ＡＩＤに着信するように、通信網に対して接続要求をすることができる。更に、１対１個別化アクセスチケットＰＡＴで指定した呼のうち、着信者が選択した１対１個別化アクセスチケットＰＡＴの呼を着信拒否することができる。また、着信者が選択した１対１個別化アクセスチケットの呼の着信拒否を解除することもできる。更に、匿名性を悪用し複数の発信者役割識別子ＡＩＤで個人攻撃を繰り返す発信者への対処として、それら複数の発信者役割識別子ＡＩＤから個人識別子ＯＩＤの同一性を判定することができ、かつ、その個人識別子をある確率で取り出すことができる。

【０２２４】次に、本発明の第２の実施形態に係るメールアクセス制御方法について図８乃至図２４を参照して説明する。上述した第１の実施形態では発信者と着信者を１対１に対応させる場合について説明したのに対して、第２の実施形態では、発信者と着信者を１対Ｎに対応させるとともに、この１対Ｎ個別化アクセスチケットの新規生成、内容変更をユーザ主導で可能とする場合について説明するものである。なお、この発信者はＰＡＴの所有者またはＰＡＴの会員のいづれかである。同様に受信者もＰＡＴの所有者またはＰＡＴの会員のいづれかである。

【０２２５】一般に、グループ通信（メーリングリスト等）の会員構成は動的に変化するため、グループ通信の主催者は会員の電話番号、Ｅメールアドレス等の連絡先情報を管理する必要がある。これに対して、第１の実施形態のように、１対１個別化アクセスチケットの新規生成しかできない場合には、連絡先情報の管理が困難である。例えば、グループを一体として管理することが困難であり、また移転制御のため、他の人に渡しても、メーリングリスト等グループ通信のアドレスとして機能しない。

【０２２６】本第２の実施形態では、このような不具合を解消するために１対Ｎ個別化アクセスチケットＰＡＴの新規生成および既存の１対Ｎ個別化アクセスチケットＰＡＴの内容変更をユーザ主導でできるようにしている。

【０２２７】まず、本第２の実施形態で使用される各識別子の定義について図８、図９を参照して説明する。

【０２２８】個人識別子（Official Identification：ＯＩＤ）は、図８（ａ）に示すように、認証局（Certificate Authority：ＣＡ）がユーザを一意に認識可能な規則に従う任意の文字列（電話番号、電子メールアドレス等）と公開鍵から構成される情報に対し、認証局ＣＡが署名したものである。

【０２２９】役割識別子（Anonymous Identification：ＡＩＤ）は、図８（ｂ）に示すように、個人識別子ＯＩＤの断片とその位置情報、冗長な文字列、ＳＣＳを動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列（ホスト名、実ドメイン名等）であるＳＣＳの情報から構成される情報に対し、認証局ＣＡが署名したものである。

【０２３０】１対Ｎ個別化アクセスチケットＰＡＴは、図８（ｃ）に示すように、２個以上の役割識別子、所有者インデックス、有効期限、移転制御フラグ、ＰＡＴ演算装置識別子から構成される情報に対し、ＰＡＴ演算装置の秘密鍵で署名したものである。

【０２３１】ここで、役割識別子ＡＩＤの１個はこのＰＡＴの所有者役割識別子ＡＩＤで、所有者ＡＩＤとこれに対応したEnabler をＰＡＴ演算装置に提示することにより、ＰＡＴへのＡＩＤの追加、ＰＡＴからのＡＩＤの削除、ＰＡＴの有効期限の変更、ＰＡＴの移転制御フラグの値の変更等、ＰＡＴに含まれる情報を変更することができる。

【０２３２】一方、ＰＡＴに含まれる所有者ＡＩＤ以外のＡＩＤはすべて会員ＡＩＤで、会員ＡＩＤとこれに対応したEnabler をＰＡＴ演算装置に提示しても、ＰＡＴに含まれる情報を変更することはできない。

【0233】所有者インデックスは、所有者ＡＩＤを識別するための数値データで、所有者ＡＩＤと会員ＡＩＤから構成されるＡＩＤリストにおける先頭のＡＩＤが所有者ＡＩＤの場合には１、先頭から２番目のＡＩＤが所有者ＡＩＤの場合には２，…、ｎ番目の場合にはｎであると定義する。移転制御フラグは、１対１個別化アクセスチケットの場合と同様、０または１の値をとりうると定義する。

【0234】所有者ＡＩＤは、ＡＩＤリストにおける所有者インデックスの値の位置に書き込まれているＡＩＤであると定義する。会員ＡＩＤは、所有者ＡＩＤ以外のすべてのＡＩＤと定義する。有効期限は、ＰＡＴの使用回数、ＰＡＴが利用不可能になる絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になる絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になってから利用不可能になるまでの相対時間（寿命）のいずれか、または複数を組み合わせて定義する。ＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）の識別子は、ＰＡＴ演算装置のシリアルナンバー（またはＰＡＴ演算オブジェクトのネットワーク上の識別名）であると定義する。ＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）の秘密鍵は、前記識別子に一意に対応すると定義する。

【0235】また、本第２の実施形態では、役割識別子ＡＩＤに対応した識別子として、Enabler を導入している。Enabler は、図９に示すように、Enabler であることを一意に表す文字列とＡＩＤから構成される情報に対して、認証局ＣＡ１が署名したものである。

【0236】次にＰＡＴの新規生成および内容変更における操作について説明する。通信端末上のセキュアなＰＡＴ演算装置、ＣＡ上もしくはＣＡから正当に依頼されたネットワーク上のＰＡＴ演算オブジェクト（以後、これもＰＡＴ演算装置と呼ぶことにする）において、次の操作が定義される。

【0237】１．ＡＩＤリストの編集

ＡＩＤとEnabler を用いて、ＰＡＴに含まれるＡＩＤのリスト（以後、ＡＩＤリストと呼ぶ）を編集する。または、ＡＩＤリストを新規生成する。

【0238】２．有効期限および移転制御フラグの設定

ＡＩＤとEnabler を用いて、ＰＡＴに含まれる有効期限の値及び移転制御フラグの値を変更する。または、新たに生成したＡＩＤリストに新たな有効期限の値及び新たな移転制御フラグの値を設定する。

【0239】所有者ＡＩＤとこの所有者ＡＩＤに対応したEnabler をＰＡＴ演算装置に提示したユーザは、ＰＡＴに含まれるＡＩＤのリストを編集できる。このとき、以下の演算規則に従う。

【0240】(1) 新規生成（MakePAT）（図１０参照）：

ＡＩＤリスト（ＡＬＩＳＴ<所有者ＡＩＤ｜会員ＡＩＤ$_1$，会員ＡＩＤ$_2$，…，会員ＡＩＤ$_n$ >）を新規生成し、生成後のＡＬＩＳＴに対し、有効期限の値および移転制御フラグの値を設定する。

【0241】

【数１】

$$AID_A + AID_B + \text{Enabler of } AID_B + \text{Enabler of } AID_A \rightarrow ALIST<AID_A \mid AID_B>$$

$$ALIST<AID_A \mid AID_B> + \text{Enabler of } AID_A + \text{有効期限の値} + \text{移転制御フラグの値} \rightarrow PAT<AID_A \mid AID_B>$$

(2) マージ（MergePAT）（図１１参照）：

同一所有者ＡＩＤの複数ＡＬＩＳＴをマージし、マージ後のＡＬＩＳＴに対し、有効期限の値および移転制御フラグの値を設定する。

【0242】

【数２】

$$ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots> + ALIST<AID_A \mid AID_{C1}, AID_{C2}, \cdots> + \text{Enabler of } AID_A \rightarrow ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots, AID_{C1}, AID_{C2}, \cdots>$$

$$ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots, AID_{C1}, AID_{C2}, \cdots> + \text{Enabler of } AID_A + \text{有効期限の値} + \text{移転制御フラグの値} \rightarrow PAT<AID_A \mid AID_{B1}, AID_{B2}, \cdots, AID_{C1}, AID_{C2}, \cdots>$$

(3) 分割（SplitPAT）（図１２参照）：

ＡＬＩＳＴを同一所有者ＡＩＤの複数ＡＬＩＳＴに分解し、分解後のすべてのＡＬＩＳＴに対し、それぞれ、有効期限の値および移転制御フラグの値を設定する。

【0243】

【数３】

$$ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots, AID_{C1}, AID_{C2}, \cdots> + \text{Enabler of } AID_A \rightarrow ALIST<AID_A \mid AID_{B1}, AID_{B2}, \cdots> + ALIST<AID_A \mid AID_{C1}, AID_{C2}, \cdots>$$

$$ALIST<AID_A \mid AID_{C1}, AID_{C2}, \cdots> + \text{Enabler of } AID_A + \text{有効期限の値} + \text{移転制御フラグの値} \rightarrow PAT<AID_A \mid AID_{C1}, AID_{C2}, \cdots>$$

(4) 所有者変更（TransPAT）（図13参照）：　　する。
ALISTの所有者AIDを変更し、変更後のALIS　　【0244】
Tに対し有効期限の値および移転制御フラグの値を設定　　【数4】

$$ALIST<AID_A \mid AID_B> + ALIST<AID_A \mid AID_{C1}, AID_{C2}, \cdots> + \text{Enabler of } AID_A + \text{Enabler of } AID_B \rightarrow ALIST<AID_B \mid AID_{C1}, AID_{C2}, \cdots>$$

$$ALIST<AID_B \mid AID_{C1}, AID_{C2}, \cdots> + \text{Enabler of } AID_B + \text{有効期限の値} + \text{移転制御フラグの値} \rightarrow PAT<AID_B \mid AID_{C1}, AID_{C2}, \cdots>$$

有効期限の値の設定における操作では、所有者AIDと　　義する。
これに対応したEnabler の両者を所有するユーザにのみ　　【0245】
有効期限の値の設定を許可するために、以下の操作を定　　【数5】

$$PAT<AID_A \mid AID_B> + \text{Enabler of } AID_A + \text{有効期限の値} \rightarrow PAT<AID_A \mid AID_B>$$

移転制御フラグの値の設定における操作では、所有者A　　下の操作を定義する。
IDとこれに対応したEnabler の両者を所有するユーザ　　【0246】
にのみ移転制御フラグの値の設定を許可するために、以　　【数6】

$$PAT<AID_A \mid AID_B> + \text{Enabler of } AID_A + \text{移転制御フラグの値} \rightarrow PAT<AID_A \mid AID_B>$$

次に、本実施形態の全体構成を示す図14～図20について説明する。図14～図20において、CAからAID$_A$ を割り当てられたユーザAは、ユーザAの計算機にAID$_A$ および Enabler of AID$_A$ を保存し、フロッピードライブ、CD－ROMドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、記憶装置及びデータ入出力機能を備える通信端末（電話、携帯電話等）に、AID$_A$ および Enabler of AID$_A$ を保存している。

【0247】同様に、CAからAID$_B$ を割り当てられたユーザBは、自らの計算機にAID$_B$ および Enabler of AID$_B$ を保存し、フロッピードライブ、CD－ROMドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、記憶装置及びデータ入出力機能を備える通信端末（電話、携帯電話等）に、AID$_B$ および Enabler of AID$_B$ を保存している。

【0248】以下、ユーザAがPAT<AID$_A$ | AID$_B$ >を生成する手順を説明する。

(1) ユーザAは、以下の手段のいずれかを用いて、AID$_B$ および Enabler of AID$_B$ を取得する。

【0249】・アノニマス・ディレクトリ・サービスADS7にAID$_B$ と Enabler of AID$_B$ を登録し、ユーザAが検索結果として取得するのを待つ（図14）。

【0250】・電子メール、シグナリング等でAID$_B$ と Enabler of AID$_B$ をユーザAに直接送信する（図15～図16）。

【0251】・フロッピーディスク、CD－ROM、MO、ICカード等の磁気、光、電子メディアにAID$_B$ と Enabler of AID$_B$ を蓄積し、ユーザAに渡す。または、ユーザAが閲覧して取得するのを待つ（図17～図18）。

【0252】・書籍、名刺等の紙メディアにAID$_B$ と Enabler of AID$_B$ を記載し、ユーザAに渡す。もしくは、ユーザAが閲覧し取得するのを待つ（図19～図20）。

【0253】(2) 上述した（1）のいずれかの手段でAID$_B$ および Enabler of AID$_B$ を取得したユーザAは、PAT演算装置に対しMakePAT命令を発行する。この手順は図14～図20で共通で、以下の通りに定義する。

【0254】(a) ユーザAは、ユーザAの通信端末にAID$_A$ 、Enabler of AID$_A$ 、AID$_B$ 、Enabler of AID$_B$ 、有効期限の値、および移転制御フラグの値をセットし、MakePAT命令の発行を要求する。

【0255】(b) ユーザAの通信端末は、MakePAT命令を生成する。

【0256】(c) ユーザAの通信端末は、生成したMakePAT命令を電子メール、シグナリング等の手段でPAT演算装置に送信する（MakePAT命令の発行）。

【0257】(d) PAT演算装置は、受信したMakePAT命令を図21、図23に従って処理し、PAT<AI

D_A | AID_B >を生成する。具体的には、

【数7】

AID_A + AID_B + Enabler of AID_B + Enabler of AID_A
→ ALIST<AID_A | AID_B >
ALIST<AID_A | AID_B > + Enabler of AID_A
+ 有効期限の値 + 移転制御フラグの値
→ PAT<AID_A | AID_B >

(e) PAT演算装置は、生成したPAT<AID_A | AID_B >を電子メール、シグナリング等の手段でユーザAの通信端末、または必要に応じて、ユーザBの通信端末に送信する。

【0258】(f) ユーザA（またはユーザB）の通信端末は、受信したPAT<AID_A | AID_B >をユーザAの通信端末の記憶装置に保存する。

【0259】PATのマージ（MergePAT、図21、図23）、PATの分割（SplitPAT、図22、図23）、PATの所有者変更（TransPAT、図21、図23）も同様の手順である。

【0260】次に、図21のフローチャートを参照して、MakePAT、MergePAT、TransPATの手順について説明する。

【0261】1．所有者AIDを指定する(ステップS4411)。

【0262】2．会員AIDをすべて指定する（ステップS4412）。

【0263】3．指定した所有者AIDと指定したすべての会員AIDからAIDリストを生成する(ステップS4413)。具体的には、任意の手段を用いて、指定した所有者AIDと指定したすべての会員AIDを連結する。

【0264】4．仮AIDと同様に、任意の手段で仮PATを生成する（ステップS4414）。

【0265】5．生成したAIDリストを生成した仮PATの定められた範囲に複写する(ステップS4415)。

【0266】6．AIDリストを複写した仮PATに、所有者インデックスの値を書き込む（ステップS4416）。

【0267】7．所有者インデックスの値を書き込んだ仮PATに、移転制御フラグの値を書き込む(ステップS4417)。

【0268】8．移転制御フラグの値を書き込んだ仮PATに、有効期限の値を書き込む（ステップS4418）。

【0269】9．有効期限の値を書き込んだ仮PATに、PAT演算装置の識別子を書き込む（ステップS4419）。

【0270】10．PAT演算装置の識別子を書き込んだ仮PATに、PAT演算装置の秘密鍵で署名する（ステップS4420）。

【0271】次に、図22のフローチャートを参照して、SplitPATの手順について説明する。

【0272】1．所有者AIDを指定する(ステップS4511)。

【0273】2．分割後のPATの会員AIDとするAIDをすべて指定する（ステップS4512）。

【0274】3．指定した所有者AIDと指定したすべての会員AIDからAIDリストを生成する（ステップS4513）。具体的には、任意の手段を用いて、指定した所有者AIDと指定したすべての会員AIDを連結する。

【0275】4．仮AIDと同様に、任意の手段で仮PATを生成する(ステップS4514)。

【0276】5．生成したAIDリストを生成した仮PATの定められた範囲に複写する（ステップ4515）。

【0277】6．AIDリストを複写した仮PATに、所有者インデックスの値を書き込む(ステップS4516)。

【0278】7．所有者インデックスの値を書き込んだ仮PATに、移転制御フラグの値を書き込む(ステップS4517)。

【0279】8．移転制御フラグの値を書き込んだ仮PATに、有効期限の値を書き込む(ステップS4518)。

【0280】9．有効期限の値を書き込んだ仮PATに、PAT演算装置の識別子を書き込む(ステップS4519)。

【0281】10．PAT演算装置の識別子を書き込んだ仮PATに、PAT演算装置の秘密鍵で署名する(ステップS4520)。

【0282】11．分割を継続する場合には（ステップS4521YES）、2．に戻り、10．までを順番に実行する。

【0283】なお、図21、図22の手順において、AIDリストの生成は、図23のフローチャートにより次のように行う。すなわち、まずバッファ長を決定し（ステップS4611）、バッファを生成する（ステップS4612）。次いで、所有者AIDを生成したバッファの空き領域にコピーする（ステップS4613）。次いで、会員AIDをバッファの空き領域にコピーし（ステップS4614）、次の会員AIDが存在すれば（ステップS4615YES）ステップS4614を繰り返す。

【0284】次に、所有者AIDの決定について説明す

る。MakePAT，MergePAT，SplitPAT，TransPAT各命令は、２個以上の引数を持ち、引数として、役割識別子ＡＩＤ、個別化アクセスチケットＰＡＴ、または、Enableを指定できると定義する。この時、ＰＡＴ演算装置は、各命令実行後に出力されるＰＡＴの所有者ＡＩＤをそれぞれ下記の規則に従い指定する。

【０２８５】・MakePATの場合

MakePAT命令に対して、第１引数から第N引数（N＝２，３，…）までＡＩＤを、第N＋１引数以降ではEnableを指定すると定義する。例えば、

MakePAT AID_1 AID_2 … AID_N Enabler of AID_1

Enabler of AID_2 … Enabler of AID_N

－ＰＡＴ演算装置は、MakePAT命令の第１引数のＡＩＤを所有者ＡＩＤであると解釈する。

【０２８６】－第N＋１引数以降のEnabler のいずれかが第１引数のＡＩＤに対応している場合に限り、ＰＡＴ演算装置はこのＡＩＤ（すなわち、第１引数のＡＩＤ）をMakePAT命令実行後に出力されるＰＡＴの所有者ＡＩＤに指定する。

【０２８７】・MergePATの場合

SplitPAT PAT_1 （AID_{11}）（AID_{21} AID_{22}）…（AID_{N1} AID_{N2} … AID_{NM}）Enabler of ＡＩＤ

－ＰＡＴ演算装置は、SplitPAT命令の第１引数のＰＡＴの所有者ＡＩＤを、SplitPAT命令実行後に出力されるＰＡＴの所有者ＡＩＤであると解釈する。

【０２９０】－第N＋１引数のEnabler が第１引数のＰＡＴの所有者ＡＩＤに対応している場合に限り、ＰＡＴ演算装置はこのＡＩＤ（すなわち、第１引数のＰＡＴの所有者ＡＩＤをSplitPAT命令実行後に出力されるＰＡＴの所有者ＡＩＤに指定する。

【０２９１】・TransPATの場合

TransPAT命令に対して、第１引数及び第２引数でＰＡＴを、第３引数でＡＩＤを、第４引数及び第５引数ではEnablerを指定すると定義する。すなわち、

TransPAT PAT_1 PAT_2 AID Enabler of AID_1 Enabler of AID_2

－ＰＡＴ演算装置は、TransPAT命令の第３引数のＡＩＤが第２引数のＰＡＴに含まれている場合に限り、第３引数のＡＩＤを、TransPAT命令実行後に出力されるＰＡＴの所有者ＡＩＤであると解釈する。

【０２９２】－第４引数のEnabler が第１引数のＰＡＴ及び第２引数のＰＡＴの両者に対応しており、かつ、第５引数のEnabler が第３引数のＡＩＤに対応している場合に限り、ＰＡＴ演算装置は第３引数のＡＩＤをTransＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤに指定する。

【０２９３】次に、会員ＡＩＤの決定について説明する。MakePAT，MergePAT，SplitPAT，TransPAT各命令の定義は上に従う。ＰＡＴ演算装置は、各命令実行後に出力されるＰＡＴの会員ＡＩＤをそれぞれ下記の規則に従い指定する。

【０２９４】・MakePATの場合

MakePAT命令実行後に出力されるＰＡＴの所有者ＡＩＤが正式に決定された場合に限り、

－ＰＡＴ演算装置は、MakePAT命令の第２引数以降のMergePAT命令に対して、第１引数から第N引数（N＝２，３，…）までＰＡＴを、第N＋１引数ではEnablerを指定すると定義する。すなわち、

MergePAT PAT PAT_1 PAT_2 … PAT_N Enabler of ＡＩＤ

－ＰＡＴ演算装置は、MergePAT命令の第１引数のＰＡＴの所有者ＡＩＤを、MergePAT命令実行後に出力されるＰＡＴの所有者ＡＩＤであると解釈する。

【０２９８】－第N＋１引数のEnabler が第１引数のＰＡＴの所有者ＡＩＤに対応している場合に限り、ＰＡＴ演算装置はこのＡＩＤ（すなわち、第１引数のＰＡＴの所有者ＡＩＤ）をMergePAT命令実行後に出力されるＰＡＴの所有者ＡＩＤに指定する。

【０２８９】・SplitPATの場合

SplitPAT命令に対して、第１引数でＰＡＴを、第２引数から第N引数（N＝３，４，…）まではあらかじめ定められた何らかの記号（この例ではカッコ（）とする）でまとめられた１個以上のＡＩＤのまとまりを、第N＋１引数ではEnableを指定すると定義する。すなわち、

SplitPAT PAT PAT_1 （AID_{11}）（AID_{21} AID_{22}）…（AID_{N1} AID_{N2} … AID_{NM}）Enabler of ＡＩＤ

－ＰＡＴ演算装置は、SplitPAT命令の第１引数のＰＡＴの所有者ＡＩＤを、SplitPAT命令実行後に出力されるＰＡＴの所有者ＡＩＤであると解釈する。

【０２９０】－第N＋１引数のEnabler が第１引数のＰＡＴの所有者ＡＩＤに対応している場合に限り、ＰＡＴ演算装置はこのＡＩＤ（すなわち、第１引数のＰＡＴの所有者ＡＩＤをSplitPAT命令実行後に出力されるＰＡＴの所有者ＡＩＤに指定する。

【０２９１】・TransPATの場合

TransPAT命令に対して、第１引数及び第２引数でＰＡＴを、第３引数でＡＩＤを、第４引数及び第５引数ではEnablerを指定すると定義する。すなわち、

TransPAT PAT_1 PAT_2 AID Enabler of AID_1 Enabler of AID_2

－ＰＡＴ演算装置は、TransPAT命令の第３引数のＡＩＤが第２引数のＰＡＴに含まれている場合に限り、第３引数のＡＩＤを、TransPAT命令実行後に出力されるＰＡＴの所有者ＡＩＤであると解釈する。

【０２９２】－第４引数のEnabler が第１引数のＰＡＴ及び第２引数のＰＡＴの両者に対応しており、かつ、第５引数のEnabler が第３引数のＡＩＤに対応している場合に限り、ＰＡＴ演算装置は第３引数のＡＩＤをTransＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤに指定する。

【０２９３】次に、会員ＡＩＤの決定について説明する。MakePAT，MergePAT，SplitPAT，TransPAT各命令の定義は上に従う。ＰＡＴ演算装置は、各命令実行後に出力されるＰＡＴの会員ＡＩＤをそれぞれ下記の規則に従い指定する。

【０２９４】・MakePATの場合

MakePAT命令実行後に出力されるＰＡＴの所有者ＡＩＤが正式に決定された場合に限り、

－ＰＡＴ演算装置は、MakePAT命令の第２引数以降のすべてのＡＩＤをMakePAT命令実行後に出力されるＰＡＴの会員ＡＩＤであると解釈する。

【０２９５】－第２引数以降のすべてのＡＩＤのうち、第N＋１引数以降で指定されたEnabler と対応しているＡＩＤのみ、ＰＡＴ演算装置はMakePAT命令実行後に出力されるＰＡＴの会員ＡＩＤに指定する。

【０２９６】・MergePATの場合

ＰＡＴ演算装置は、MergePAT命令実行後に出力されるＰＡＴの所有者ＡＩＤが正式に決定された場合に限り、MergePAT命令の第１引数から第N引数で指定されたすべてのＰＡＴの会員ＡＩＤを、MergePAT命令実行後に出力されるＰＡＴの会員ＡＩＤに指定する。

【０２９７】・SplitPATの場合

ＰＡＴ演算装置は、SplitPAT命令実行後に出力されるＰＡＴの所有者ＡＩＤが正式に決定された場合に限り、SplitPAT命令の第１引数で指定されたＰＡＴの会員ＡＩＤを、SplitPAT命令実行後に出力されるＰＡＴの会員ＡＩＤに指定する。このとき、会員ＡＩＤはカッコ（）単位で別々のＰＡＴに振り分けられる。例え

ば、

SplitPAT PAT(AID_{11}) (AID_{21} AID_{22})…
(AID_{N1} AID_{N2} … AID_{NM}) Enabler of AID

の場合、(AID_{11})と(AID_{21} AID_{22})と(AID_{N1} AID_{N2} … AID_{NM})は所有者ＡＩＤが共通な別のＰＡＴの会員ＡＩＤになる。

【０２９８】・TransＰＡＴの場合

ＰＡＴ演算装置は、TransＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤが正式に決定された場合に限り、TransＰＡＴ命令の第１引数で指定されたＰＡＴのすべての会員ＡＩＤ及び第２引数で指定されたＰＡＴの会員ＡＩＤのうち新所有者ＡＩＤとなる予定の会員ＡＩＤを除いた残りのすべての会員ＡＩＤを、TransＰＡＴ命令実行後に出力されるＰＡＴの会員ＡＩＤに指定する。

【０２９９】次に、Enabler の正当性の検証について説明する。このEnabler の正当性の検証は、MakeＰＡＴ、MergeＰＡＴ、SplitＰＡＴ、TransＰＡＴで共通であり、図２４に示すように行われる。

【０３００】１．ＡＩＤとEnabler を入力する（ステップＳ５５１１）。

【０３０１】２．この入力されたＡＩＤとEnabler をそれぞれ認証局ＣＡの公開鍵で検証する（ステップＳ５５１２）。少なくとも一方が改竄されている場合には(ステップＳ５５１３ＹＥＳ)、処理を終了する。

【０３０２】３．Enabler であることを証明する文字列を入力する（ステップＳ５５１４）。

【０３０３】４．ステップＳ５５１１のEnabler の先頭フィールドとステップＳ５５１４の文字列を比較する（ステップＳ５５１５）。一致しない場合には(ステップＳ５５１６ＮＯ)、処理を終了する。

【０３０４】５．一致する場合には(ステップＳ５５１６ＹＥＳ)、ステップＳ５５１１のＡＩＤとEnabler 中のＡＩＤを比較する（ステップＳ５５１７）。

【０３０５】６．比較結果を出力する(ステップＳ５５１９)。

【０３０６】次に、図２５～図２８を参照して、本発明の第３の実施形態について説明する。

【０３０７】上述した実施形態における個別化アクセスチケット（ＰＡＴ）の新規生成（MakeＰＡＴ）および所有者変更（TransＰＡＴ）では、会員ＡＩＤと Enabler of会員ＡＩＤを個別化アクセスチケットの所有者に渡すことが必要であるが、これを所有者に渡すと、その所有者が別の所有者の主催するグループ通信に対して、取得した会員ＡＩＤで参加することが可能になる。すなわち、会員ＡＩＤを用いた成りすましが可能になるという問題がある。また、その所有者が取得した会員ＡＩＤおよび Enabler of 会員ＡＩＤを不特定多数が閲覧可能なメディアに掲載すれば、誰でもその会員ＡＩＤにアクセス可能になるため、会員ＡＩＤのユーザへの嫌がらせが発生する恐れがあるとともに、また第三者による会員ＡＩＤを用いた成りすましも可能になるという問題がある。

【０３０８】そこで、本実施形態では、 Enabler of 会員ＡＩＤを所有者に渡さなくても、MakeＰＡＴおよびTransＰＡＴを可能にする。

【０３０９】このために、本実施形態では、Ｎｕｌｌ－ＡＩＤ（AID_{Null}）および該Ｎｕｌｌ－ＡＩＤの Enabler(Enabler of Ｎｕｌｌ－ＡＩＤまたは Enabler of AID_{Null}）を使用して、個別化アクセスチケット（ＰＡＴ）の新規生成および既存の個別化アクセスチケット（ＰＡＴ）の内容変更を行うものである。ここで、Ｎｕｌｌ－ＡＩＤを含む演算は、以下のすべての規則に従う：

(a) 上述した実施形態における新規生成（MakeＰＡＴ）、マージ（MergeＰＡＴ）、分割（SplitＰＡＴ）、変更（TransＰＡＴ）からなる演算規則、(b) Ｎｕｌｌ－ＡＩＤにのみ適用可能な規則として、ｉ．Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知であり、ii． Enabler of Ｎｕｌｌ－ＡＩＤは、すべてのユーザに既知である。

【０３１０】ここで、上述した実施形態で定義した演算規則について説明する。

【０３１１】(1) 複数ＡＩＤからＰＡＴを作る（MakeＰＡＴ）：

【数８】

$$AID_{holder} + AID_{member1} + AID_{member2} + \cdots + AID_{memberN} + \text{Enabler of } AID_{member1} + \text{Enabler of } AID_{member2} + \cdots + \text{Enabler of } AID_{memberN} + \text{Enabler of } AID_{holder} \rightarrow PAT<AID_{holder} \mid AID_{member1}, AID_{member2}, \cdots, AID_{memberN}>$$

【数９】

(2) 同一所有者の複数ＰＡＴをマージする（MergeＰＡＴ）：

$$PAT<AID_{holder} \mid AID_{membera1}, AID_{membera2}, \cdots, AID_{memberaM}> + PAT<AID_{holder} \mid AID_{memberb1}, AID_{memberb2}, \cdots,$$

$AID_{memberbN}>$
+ Enabler of AID_{holder}
→ $PAT<AID_{holder} | AID_{membera1}, AID_{membera2}, \cdots, AID_{meberaM}, AID_{memberb1}, AID_{memberb2}, \cdots, AID_{memberbN}>$

(3) PATを同一所有者の複数PATに分割する（SplitPAT）：

【数10】

$PAT<AID_{holder} | AID_{membera1}, AID_{membera2}, \cdots, AID_{meberaM}, AID_{memberb1}, AID_{memberb2}, \cdots, AID_{memberbN}>$
+ Enabler of AID_{holder}
→ $PAT<AID_{holder} | AID_{membera1}, AID_{membera2}, \cdots, AID_{meberaM}>$ + $PAT<AID_{holder} | AID_{memberb1}, AID_{memberb2}, \cdots, AID_{memberbN}>$

(4) PATの所有者AIDを変更する（TransPAT）：

【数11】

$PAT<AID_{holder} | AID_{membera1}, AID_{membera2}, \cdots, AID_{meberaM}> + PAT<AID_{holder} | AID_{newholder}>$
+ Enabler of AID_{holder} + Enabler of $AID_{newholder}$
→ $PAT<AID_{newholder} | AID_{membera1}, AID_{membera2}, \cdots, AID_{meberaM}>$

Null-AIDを含むPATへの有効期限の値及び移転制御フラグの値の指定方法は、上述した第2の実施形態における有効期限の値及び移転制御フラグの値の指定方法に従う。

【0312】次に、Null-AIDに関する演算例について説明する。

【数12】

$AID_{Null} + AID_A$ + Enabler of AID_A + Enabler of AID_{Null}
→ $PAT<AID_{Null} | AID_A>$

(2) $PAT<AID_{Null} | AID_A>$と$PAT<AID_{Null} | AID_B>$とから$PAT<AID_{Null} | AID_A, AID_B>$を作る場合：

(a) Null-AIDの規則(b)i. および(b)ii.より、

$PAT<AID_{Null} | AID_A> + PAT<AID_{Null} | AID_B>$
+ Enabler of AID_{Null}
→ $PAT<AID_{Null} | AID_A, AID_B>$

(3) $PAT<AID_{Null} | AID_A>$と$PAT<AID_{Null} | AID_B>$と Enabler of AID_A とから$PAT<AID_A | AID_B>$を作る場合：

(a) Null-AIDの規則(b)i. および(b)ii.より、

$PAT<AID_{Null} | AID_A> + PAT<AID_{Null} | AID_B>$
+ Enabler of AID_{Null} + Enabler of AID_A
→ $PAT<AID_A | AID_B>$

Null-AIDのデータ構造は、図25に示すように、Null-AIDであることを一意に表す文字列（例えば、この文字列は認証局CAで定義される）および該文字列に対して認証局CAの署名を施したもので構成される。

【0317】また、Enabler of Null-AIDのデータ構造は、図26に示すように、Enablerであることを一意に表す文字列（例えば、この文字列は認証局CAで定義される）、Null-AIDの実体、および前記Enablerであることを表す文字列と前記Null-AIDの実体を連結した文字列に対して認証局CAの署名を施したもので構成される。

【0313】(1) AID_A と Enabler of AID_A とから$PAT<AID_{Null} | AID_A>$を作る場合：

(a) Null-AIDの規則(b)i. および(b)ii.より、AID_{Null}と Enabler of AID_{Null}は既知である。

【0314】(b) MakePATにより

【数12】

AID_{Null}と Enabler of AID_{Null}は既知である。

【0315】(b) MergePATにより

【数13】

AID_{Null}と Enabler of AID_{Null}は既知である。

【0316】(b) TransPATにより

【数14】

【0318】なお、Ｎｕｌｌ－ＡＩＤおよび Enabler of Ｎｕｌｌ－ＡＩＤは、セキュアなＰＡＴ演算装置およびセキュアなＰＡＴ認証局で保持される。

【0319】次に、本実施形態の第１の応用例について図２７を参照して説明する。図２７においては、以下の動作を行う。

【0320】(1) ユーザＢ（ＰＡＴ会員）は、ユーザＢの端末と接続されたセキュアなＰＡＴ演算装置で前記Ｎｕｌｌ－ＡＩＤに関する演算例（１）を実行してＰＡＴ＜AID_{Null}｜AID_B＞を生成し、任意の手段でユーザＡ（ＰＡＴ所有者）に渡す。

【0321】(2) ＰＡＴ＜AID_{Null}｜AID_B＞を受信したユーザＡは、ユーザＡの端末に接続されたセキュアなＰＡＴ演算装置で

(a) Ｎｕｌｌ－ＡＩＤに関する演算例（１）を実行してＰＡＴ＜AID_{Null}｜AID_A＞を作る。

【0322】(b) Ｎｕｌｌ－ＡＩＤに関する演算例（３）を実行してＰＡＴ＜AID_A｜AID_B＞を作る。

【0323】(3) ユーザＡは、生成したＰＡＴ＜AID_A｜AID_B＞を任意の手段でユーザＢに渡す。

【0324】なお、有効期限の決定方法は前述した方法と共通のため省略する。また、Ｎｕｌｌ－ＡＩＤに関する演算の処理は前述した方法と共通のため省略する。

【0325】ＰＡＴ＜AID_{Null}｜AID_A，AID_B＞をユーザＢに渡す場合には、上述した動作（２）において、前記Ｎｕｌｌ－ＡＩＤに関する演算例（２）を実行する。

【0326】次に、本実施形態の第２の応用例について図２８を参照して説明する。図２８においては、以下の動作を行う。

【0327】(1) ユーザＢ（ＰＡＴ会員）は、ユーザＢの端末と接続されたセキュアなＰＡＴ演算装置でＮｕｌｌ－ＡＩＤに関する演算例（１）を実行してＰＡＴ＜AID_{Null}｜AID_B＞を作り、任意の公開情報とともにアノニマス・ディレクトリ・サービスＡＤＳに登録する。

【0328】(2) ユーザＡ（ＰＡＴ所有者）は、ユーザＡの端末に接続されたセキュアなＰＡＴ演算装置でＮｕｌｌ－ＡＩＤに関する演算例（１）を実行してＰＡＴ＜AID_{Null}｜AID_A＞を作り、任意の検索条件とともにアノニマス・ディレクトリ・サービスＡＤＳに提示する。

【0329】(3) ユーザＢの個人情報がユーザＡの提示した検索条件を満足した場合、アノニマス・ディレクトリ・サービスＡＤＳに接続されたセキュアなＰＡＴ演算装置は

(a) Ｎｕｌｌ－ＡＩＤに関する演算例（２）を実行してＰＡＴ＜AID_{Null}｜AID_A，AID_B＞を作る。

【0330】(b) ＰＡＴ＜AID_{Null}｜AID_A，AID_B＞をアノニマス・ディレクトリ・サービスＡＤＳに渡す。

【0331】(4) アノニマス・ディレクトリ・サービスＡＤＳは、ＰＡＴ演算装置で作られたＰＡＴ＜AID_{Null}｜AID_A，AID_B＞をユーザＡに渡す。

【0332】(5) ＰＡＴ＜AID_{Null}｜AID_A，AID_B＞を受け取ったユーザＡは、ユーザＡの端末に接続されたセキュアなＰＡＴ演算装置で下記のTransＰＡＴ演算を実行して、ＰＡＴ＜AID_A｜AID_B＞を作る。

【0333】

【数15】

$$PAT\langle AID_{Null} \mid AID_A \rangle + PAT\langle AID_{Null} \mid AID_A, AID_B \rangle + \text{Enabler of } AID_{Null} + \text{Enabler of } AID_A \rightarrow PAT\langle AID_A \mid AID_B \rangle$$

尚、有効期限の決定方法は前述した方法と共通のため省略する。また、Ｎｕｌｌ－ＡＩＤに関する演算の処理は前述した方法と共通のため省略する。

【0334】ＰＡＴ＜AID_A｜AID_B＞をアノニマス・ディレクトリ・サービスＡＤＳに接続されたセキュアなＰＡＴ演算装置で生成する場合には、そのＰＡＴ演算装置に Enabler of AID_A を渡す。そして、上述した動作（３）において、Ｎｕｌｌ－ＡＩＤに関する演算例（３）を実行する。

【0335】ＰＡＴ＜AID_B｜AID_A＞をアノニマス・ディレクトリ・サービスＡＤＳに接続されたセキュアなＰＡＴ演算装置で生成して、ユーザＢに渡す場合には、そのＰＡＴ演算装置に Enabler of AID_B を渡す。そして、上述した動作（３）において、Ｎｕｌｌ－ＡＩＤに関する演算例（３）と同様の演算を実行する。

【0336】次に、本発明の第４の実施形態について図２９～図３１を参照して説明する。グループ通信においては参加者を固定したい状況はしばしば発生するが、上述した実施形態では個別化アクセスチケット（ＰＡＴ）を変更不可にする機能を持たないため、参加者を固定することができない。すなわち、上述した実施形態では、参加者を固定するか否かは、個別化アクセスチケットの所有者の判断に一任されている。

【0337】そこで、本実施形態では、個別化アクセスチケットに読取専用属性を設定している。

【0338】このため、本実施形態では、Ｇｏｄ－ＡＩＤ（AID_{God}）を用いて、個別化アクセスチケット（ＰＡＴ）に読取専用属性を設定している。ここで、Ｇｏｄ－ＡＩＤに関する演算は、以下のすべての規則に従う：

(a) Ｇｏｄ－ＡＩＤは、すべてのユーザに既知であり、

(b) Ｇｏｄ－ＡＩＤに関する演算は、以下のいずれかのみ許可される：

【数16】

i．AID_{holder}がAID_{Null}でもAID_{God}でもない場合：

$PAT<AID_{holder} | AID_{member1}, AID_{member2}, \cdots, AID_{memberN}>$
+ Enabler of AID_{holder}
→ $PAT<AID_{God} | AID_{holder}, AID_{member1}, AID_{member2}, \cdots, AID_{memberN}>$

ii．AID_{holder}がAID_{Null}の場合：

$PAT<AID_{Null} | AID_{member1}, AID_{member2}, \cdots, AID_{memberN}>$
+ Enabler of AID_{Null}
→ $PAT<AID_{God} | AID_{member1}, AID_{member2}, \cdots, AID_{memberN}>$

God－AIDのデータ構造は、図29に示すように、God－AIDであることを一意に表す文字列（例えば、この文字列は認証局CAで定義される）および該文字列に対して認証局CAの署名を施したものから構成される。God－AIDは、上述したセキュアなPAT演算装置およびセキュアなPAT認証局で保持されている。

【0339】Null－AIDを含むPATの処理は、図21－図24に従う。所有者AIDがNull－AIDでもGod－AIDでもない場合には、AIDリストにGod－AIDを付加し、所有者インデックスの値をGod－AID付加後のAIDリストにおけるGod－AIDの位置と等しくなるように指定する。所有者AIDがNull－AIDの場合には、AIDリストからNull－AIDを削除し、次にGod－AIDを付加し、最後に所有者インデックスの値をGod－AID付加後のAIDリストにおけるGod－AIDの位置と等しくなるように指定する。

【0340】次に、本実施形態の応用例について図30を参照して説明する。

【0341】$PAT<AID_{Null} | AID_A>$と$PAT<AID_{Null} | AID_B>$とから$PAT<AID_{God} | AID_A, AID_B>$を作る場合、PAT所有者（図30におけるユーザA）の端末に接続されたセキュアなPAT演算装置において、以下の演算を実行する。

【0342】(1) 上述したMergePATにより

【数17】

$$PAT<AID_{Null} | AID_A> + PAT<AID_{Null} | AID_B> + Enabler\ of\ AID_{Null} \rightarrow PAT<AID_{Null} | AID_A, AID_B>$$

(2) God－AIDに関する演算規則（a）より、AID_{God}は既知である。

(3) God－AIDに関する演算規則(b)ii.より

【数18】

$$PAT<AID_{Null} | AID_A, AID_B> + Enabler\ of\ AID_{Null} \rightarrow PAT<AID_{God} | AID_A, AID_B>$$

上記演算は、第三者の計算機（サーチエンジンなど）に接続されたセキュアなPAT演算装置（図31）またはセキュアなPAT認証局でも実行される。

【0343】次に、図32を参照して、本発明の第5の実施形態について説明する。

【0344】上述した第3の実施形態で説明したようにNull－AIDを追加すると、以下に説明するように、個別化アクセスチケット（PAT）の所有者（所有者AIDのユーザ）が会員（会員AIDのユーザ）へのアクセス権を第三者に譲渡できるようになるという問題がある。しかも、会員に無断で譲渡可能である。

【0345】1．$PAT<AID_A | AID_B>$の所有者Aが（会員はB）

・$PAT<AID_A | AID_B>$
・AID_A
・Enabler of AID_A

を用いて、$PAT<AID_{Null} | AID_B>$を作る。ここで、Aは、$PAT<AID_A | AID_B>$に加えて

・AID_A
・Enabler of AID_A
・AID_{Null}
・Enabler of AID_{Null}

をすべて知っているとする。

【0346】(a) Aは、MakePATにより、$PAT<AID_A | AID_{Null}>$を作る。

【0347】

【数19】

$$AID_A + AID_{Null} + Enabler\ of\ AID_{Null} + Enabler\ of\ AID_A \rightarrow PAT<AID_A | AID_{Null}>$$

(b) Aは、TransPATにより、$PAT<AID_{Null} | AID_B>$を作る。

【0348】

【数20】

$$PAT<AID_A \mid AID_B> + PAT<AID_A \mid AID_{Null}> + Enabler\ of\ AID_A + Enabler\ of\ AID_{Null} \rightarrow PAT<AID_{Null} \mid AID_B>$$

上記1．(b) の後、AがPAT<AID$_{Null}$ | AID$_B$ >を第三者Cに渡すと次の2．が可能となる。

【0349】2．Cは、PAT<AID$_{Null}$ | AID$_B$ >を用いて、PAT<AID$_C$ | AID$_B$ >を作る。ここで、Cは、PAT<AID$_{Null}$ | AID$_B$ >に加えて

・AID$_C$

・Enabler of AID$_C$

をすべて知っているとする。

【0350】(a) Cは、MakePATにより、PAT<AID$_{Null}$ | AID$_C$ >を作る。

【0351】

【数21】

$$AID_{Null} + AID_C + Enabler\ of\ AID_C + Enabler\ of\ AID_{Null} \rightarrow PAT<AID_{Null} \mid AID_C>$$

【0352】

(b) Cは、TransPATにより、PAT<AID$_C$ | AID$_B$ >を作る。

【数22】

$$PAT<AID_{Null} \mid AID_B> + PAT<AID_{Null} \mid AID_C> + Enabler\ of\ AID_{Null} + Enabler\ of\ AID_C \rightarrow PAT<AID_C \mid AID_B>$$

上記2(b) の結果、CはPAT<AID$_C$ | AID$_B$ >を得るので、Bへのアクセスが可能になる。

【0353】そこで、本実施形態では、PAT<AID$_{holder}$ | AID$_{member}$>の所有者がAID$_{member}$のEnabler を知らない場合には、このPATからPAT<AID$_{Null}$ | AID$_{member}$>を作ることができないようにする。

【0354】上述した第3の実施形態では、PATの所有者がAID$_{member}$のEnabler なしでPAT<AID$_{Null}$ | AID$_{member}$>を作るためには、PAT<AID$_{holder}$ | AID$_{Null}$>を作ることが必要になる。

【0355】そこで、本実施形態では、上述した第3の実施形態で説明したNull-AIDに対して、以下の規則を追加する。

【0356】Null-AIDはPATの所有者AIDとしてのみ使用できる（会員AIDとしては使用できない）。

【0357】・PAT<AID$_{Null}$ | AID$_{member1}$, AID$_{member2}$, …, AID$_{memberN}$ >は許可する。

【0358】・PAT<AID$_{holder}$ | AID$_{Null}$, AID$_{member1}$, AID$_{member2}$, …, AID$_{memberN}$ >は許可しない。

【0359】上述した実施形態におけるセキュアなPAT演算装置とセキュアなPAT認証局にそれぞれNull-AIDが会員AIDに含まれているか否かをチェックする機能を追加する。この会員AIDのチェック処理機能について図32に示すフローチャートを参照して説明する。

【0360】1．Null-AIDとPATを入力する（ステップS6911）。

【0361】2．ステップS6911で入力したPATから、会員AIDをすべて取り出す（ステップS6913）。

【0362】3．この取り出したすべての会員AIDについて、それぞれ、ステップS6911で入力したNull-AIDと比較する（ステップS6915）。

【0363】・すべての会員AIDがNull-AIDと完全に一致しない場合（ステップS6917NO、S6919NO）、MergePAT、SplitPAT、またはTransPAT処理に移る（図21または図22）（ステップS6921）。

【0364】・会員AIDが1つでもNull-AIDと完全に一致する場合（ステップS6917YES）、処理を終了する。

【0365】次に、図33～図39を参照して、本発明の第6の実施形態について説明する。この第6の実施形態は、上述した第1の実施形態において図2に示した役割識別子AIDに対して図34（b）のようにリンク情報を追加するとともに、図2に示した1対1個別化アクセスチケットPATに含まれていた役割識別子AIDの実体の代わりに前記役割識別子AIDのリンク情報を図34（c）に示すように設定し、該リンク情報で役割識別子AIDを一意に特定するように構成した点が異なるものである。

【0366】なお、このようにリンク情報を追加された役割識別子AIDをリンク情報付き役割識別子AIDと称し、AIDのリンク情報を有する1対1個別化アクセスチケットPATをリンク指定型1対1個別化アクセスチケットPATと称することにする。また、リンク情報は、役割識別子AIDを一意に特定可能な情報であり、一般に識別子と呼ばれる種類のデータで、例えば認証局CAによって役割識別子AIDに対して一意に付与されるシリアル番号である。

【0367】まず、図33を参照して、本発明の第6の

実施形態の全体構成図について説明する。図３３において、１は認証局ＣＡであり、個人識別子ＯＩＤの認証権限と役割識別子ＡＩＤの発行権限を有し、ユーザに対して役割識別子を割り当てる機能を有する。３はユーザであり、５はセキュア・コミュニケーション・サービスＳＣＳであり、ユーザ３間の電子メールを転送し、必要に応じて着信拒否および個人識別子の同一性を判定し、取り出す。７はアノニマス・ディレクトリ・サービスＡＤＳであり、役割識別子ＡＩＤ、移転制御フラグの値、有効期限の値、および、公開情報を管理するデータベースである。すなわち、アノニマス・ディレクトリ・サービスＡＤＳ７は、検索者の役割識別子ＡＩＤと検索条件を満足する登録者の役割識別子ＡＩＤから個別化アクセスチケットＰＡＴを生成し、検索者に発行する機能を有する。

【０３６８】ユーザの要求に基づいて個人識別子から役割識別子ＡＩＤを生成し、そのユーザに割り当てるまでの一連の処理はリンク情報が付加されることを除いて第１の実施形態と基本的に同じであるが、具体的に図３４を参照して説明する。

【０３６９】図３４は、個人識別子ＯＩＤ(Official Identification)とリンク情報付き役割識別子ＡＩＤとリンク指定型１対１個別化アクセスチケットＰＡＴの例を示している。個人識別子ＯＩＤは、図３４（ａ）に示すように、認証局ＣＡ１がユーザを一意に識別可能な規則に従う任意の文字列と公開鍵から構成される情報に対し、認証局ＣＡ１が署名したものである。また、リンク情報付き役割識別子ＡＩＤは、図３４（ｂ）に示すように、個人識別子ＯＩＤの断片とその位置情報、冗長な文字列、ＳＣＳを動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列（ホスト名、実ドメイン等）、およびリンク情報から構成される情報に対し、認証局ＣＡ１が署名したものである。

【０３７０】また、リンク指定型１対１個別化アクセスチケットＰＡＴは、図３４（ｃ）に示すように、移転制御フラグ、役割識別子AID_0のリンク情報、役割識別子AID_1のリンク情報、有効期限から構成される情報に対してアノニマス・ディレクトリ・サービスＡＤＳが署名したものである。

【０３７１】ユーザ３がリンク情報付き役割識別子ＡＩＤを認証局ＣＡ１に対して要求する処理は、第１の実施形態において前述したものと同じである。

【０３７２】次に、上述した役割識別子ＡＩＤの要求に対する認証局ＣＡ１が役割識別子ＡＩＤをユーザ３に対して交付する処理も第１の実施形態において前述したものと同じである。

【０３７３】次に、認証局ＣＡにおけるリンク情報付き役割識別子ＡＩＤの生成処理について図３５を参照して説明する。図３５において、認証局ＣＡは個人識別子ＯＩＤの全長Ｌと等しい長さの情報を生成する。この情報を仮の役割識別子ＡＩＤとする（ステップＳ７２１１）。次に、個人識別子ＯＩＤの部分複写を行うために、個人識別子ＯＩＤの複写範囲を指定するパラメータp_iとl_iの値をそれぞれ乱数発生等の任意の手段を用いて決定する（ステップＳ７２１３）。ここで、Ｌは個人識別子ＯＩＤの全長と等しく、l_iは$0 \leqq l_i \leqq L$の関係が成立する範囲で任意に定めた値とする。次に、個人識別子ＯＩＤの先頭から位置p_iから位置$p_i + l_i$の範囲の情報を、仮ＡＩＤの同じ位置に複写する（ステップＳ７２１５）。つまり、このＯＩＤ断片は仮ＡＩＤの先頭から位置p_iと位置$p_i + l_i$の範囲に複写される。次に、ＯＩＤを部分複写した仮ＡＩＤの定められた範囲に、p_iとl_iの値を任意の手段で暗号化して書き込む（ステップＳ７２１７）。次に、これらの値を書き込んだ仮ＡＩＤの定められた範囲にセキュア・コミュニケーション・サービスＳＣＳ５を動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列（ホスト名、実ドメイン名等）を書き込む（ステップＳ７２１９）。次に、リンク情報を付加する（ステップＳ７２２０）。そして、このように文字列およびリンク情報を書き込んだ仮ＡＩＤに認証局ＣＡ１の秘密鍵で署名する（ステップＳ７２２１）。

【０３７４】次に、ユーザＢ３の役割識別子ＡＩＤ及び公開情報をアノニマス・ディレクトリ・サービスＡＤＳ７に登録する手続きについて説明する。登録者であるユーザＢ３とアノニマス・ディレクトリ・サービスＡＤＳ７との間で、ユーザＢ３の役割識別子ＡＩＤとＡＤＳ７の証明書を用いて、任意の手段で双方向認証を行う。次に、ユーザＢ３は、移転制御フラグの値、有効期限の値、及び、趣味などの公開情報をＡＤＳ７に送信する。次に、ＡＤＳ７はユーザＢ３から受信した移転制御フラグの値、有効期限の値、すべての公開情報を、すべてユーザＢ３のＡＩＤと関連付けて記憶装置に記録する。

【０３７５】なお、上記手続きにおいて、登録者であるユーザＢ３とＡＤＳ７間の通信を暗号化する場合もある。

【０３７６】次に、ユーザＡ３がアノニマス・ディレクトリ・サービスＡＤＳ７に登録された公開情報を検索する手続きについて説明する。検索者であるユーザＡ３とアノニマス・ディレクトリ・サービスＡＤＳ７との間で、ユーザＡ３のＡＩＤとＡＤＳ７の証明書を用いて、任意の手段で双方向認証を行う。次に、ユーザＡ３は、任意の検索条件をアノニマス・ディレクトリ・サービスＡＤＳ７に送信する。次に、アノニマス・ディレクトリ・サービスＡＤＳ７は、受信したすべての検索条件を記憶装置に提示し、これらの検索条件を満足する登録者の役割識別子ＡＩＤを抽出する。次に、アノニマス・ディレクトリ・サービスＡＤＳ７はユーザＡ３の役割識別子ＡＩＤのリンク情報と検索条件を満足した登録者の役割識別子ＡＩＤのリンク情報と移転制御フラグの値と有効

期限の値からリンク指定型１対１個別化アクセスチケットＰＡＴを生成する。次に、ＡＤＳ７は、生成したＰＡＴをユーザＡ３に送信する。

【０３７７】なお、上記手続きにおいて、検索者であるユーザＡ３とＡＤＳ７間の通信を暗号化する場合もある。

【０３７８】リンク指定型１対１個別化アクセスチケットは、アノニマス・ディレクトリ・サービスＡＤＳ７の検索結果として生成する。

【０３７９】次に、図３６のフローチャートを参照して、ＡＤＳにおけるリンク指定型１対1個別化アクセスチケットＰＡＴの生成処理について説明する。まず、ある定められた長さの情報を生成する。これを仮の個別化アクセスチケット（仮ＰＡＴ）とする(ステップＳ７５１０）。次に、検索者であるユーザＡ３の役割識別子ＡＩＤのリンク情報と登録者であるユーザＢ３の役割識別子ＡＩＤのリンク情報を仮ＰＡＴの定められた範囲に複写する（ステップ７５１６）。次に、移転制御フラグの値と有効期限の値をそれぞれ、ＡＩＤのリンク情報を複写した仮ＰＡＴの定められた範囲に書き込む（ステップＳ７５１７）。次に、これらの値を書き込んだ仮ＰＡＴにＡＤＳの秘密鍵で署名する（ステップＳ７５１９）。

【０３８０】次に、リンク指定型１対１個別化アクセスチケットＰＡＴによる移転制御について説明する。移転制御とは、ＰＡＴを譲渡されたあるいは盗聴した第三者（本来はアクセス権を有していないユーザ）から、正当なアクセス権を持つユーザへのアクセスを制限する機能である。

【０３８１】アノニマス・ディレクトリ・サービスＡＤＳ７及び登録者ＡＩＤのユーザＢ３は、個別化アクセスチケットＰＡＴの移転制御フラグにある値を設定することにより、アクセス権を有していない第三者からのユーザＢ３への接続を禁止することができる。

【０３８２】移転制御フラグの値を１に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５と発信者の間で任意のチャレンジ／レスポンス方式に従い発信者役割識別子ＡＩＤを認証するため、発信者が発信者ＡＩＤとＰＡＴの両者を発信者以外のいかなるユーザに渡しても、そのユーザは登録者にＳＣＳ５を介して接続できない。

【０３８３】一方、移転制御フラグの値を０に設定した場合には、ＳＣＳ５と発信者との間でいかなるチャレンジ／レスポンスも行わないため、発信者が発信者ＡＩＤとＰＡＴの両者を発信者以外のユーザに渡したら、それらのユーザもアノニマス・ディレクトリ・サービスの登録者とＳＣＳ５を介して接続できるようになる。

【０３８４】次に、図３７を参照してＳＣＳにおけるメールアクセス制御方法について説明する。

【０３８５】発信者はＦｒｏｍ：行に”発信者ＡＩＤ@発信者のＳＣＳの実ドメイン”、Ｔｏ：行に”ＰＡＴ@発信者のＳＣＳの実ドメイン”の形式で指定する。

【０３８６】ＳＣＳはＳＭＴＰ(Simple Mail Transfer Protocol)等のＭＴＡ(Message Transfer Agent)の受信したメールを取得し、図３７に示す処理を実行する。

【０３８７】１．ＰＡＴの署名をＡＤＳの公開鍵を用いて検証する(ステップ７７１３）。

【０３８８】・ＰＡＴの署名に改竄が認められる場合（ステップＳ７７１５ＹＥＳ）、メールを破棄して終了する(ステップＳ７７１６）。

【０３８９】・ＰＡＴの署名に改竄が認められない場合(ステップＳ７７１５ＮＯ）、下記処理２．を実行する。

【０３９０】２．発信者ＡＩＤのリンク情報をＰＡＴに提示して検索する（ステップＳ７７１７、Ｓ７７２０、Ｓ７７２２）。

【０３９１】・発信者ＡＩＤのリンク情報と完全一致するリンク情報がＰＡＴに含まれていない場合には（ステップＳ７７２３ＮＯ）、メールを破棄して終了する（ステップＳ７７１６）。

【０３９２】・発信者ＡＩＤのリンク情報と完全一致するリンク情報がＰＡＴに含まれている場合には（ステップＳ７７２３ＹＥＳ）、下記処理３．を実行する。

【０３９３】３．ＰＡＴの有効期限の値を評価する（ステップＳ７７２５、Ｓ７７２７）。

【０３９４】・ＰＡＴが有効期間外の場合には（ステップＳ７７２７ＮＯ）、メールを破棄して終了する（ステップＳ７７１６）。

【０３９５】・ＰＡＴが有効期限内の場合には（ステップＳ７７２７ＹＥＳ）、下記処理４．を実行する。

【０３９６】４．ＰＡＴの移転制御フラグの値を参照して、発信者を認証するか否かを決定する（ステップＳ７７３１、Ｓ７７３３）。

【０３９７】・値が１の場合には（ステップＳ７７３３ＹＥＳ）、ＳＣＳはリンク情報を認証局ＣＡに提示して発信者ＡＩＤの実体及び発信者ＡＩＤの公開鍵を取得し、ＳＣＳと発信者との間でチャレンジ／レスポンス認証を実行して、発信者の署名を確認する（ステップＳ７７３５）。署名が正しい場合には、着信者を指定し、ＰＡＴを添付する（ステップＳ７７３７）。署名が正しくない場合には、メールを廃棄して終了する（ステップＳ７７１６）。

【０３９８】・値が０の場合には（ステップＳ７７３３ＮＯ）、チャレンジ／レスポンス認証を実行せずに着信者を指定し、ＰＡＴを添付する（ステップＳ７７３７）。

【０３９９】ＳＣＳと発信者との間のチャレンジ／レスポンス方法は１対１個別化アクセスチケットに対するチャレンジ／レスポンス方法と同様である。

【０４００】次に、ＳＣＳにおける着信者の指定方法について説明する。

【0401】SCSは、まず、発信者AIDのリンク情報をPATに提示して検索し、発信者AIDのリンク情報と完全一致しないすべてのリンク情報を取得する。次に、取得したすべてのリンク情報を認証局CAに提示して検索し、AIDを取得する。取得したすべてのAIDを以後、着信者AIDと定義する。次に、取得したすべてのAIDについて、それぞれ、着信者AIDから着信者のSCSの実ドメインを取り出す。次に、着信者を"着信者AID@着信者のSCSの実ドメイン"の形式で指定する。最後に、SCSは発信者を"発信者AID@発信者のSCSの実ドメイン"の形式から"発信者AID"の形式に変更する。

【0402】SCSにおけるPATの添付方法は、1対1個別化アクセスチケットに対する添付方法と同様である。

【0403】次に、SCSにおけるリンク指定型1対1個別化アクセスチケットPATに対する着信拒否方法について説明する。

【0404】着信拒否の設定：ユーザとセキュア・コミュニケーション・サービスSCS5との間で、任意の手段で双方向認証を行う。次に、ユーザは登録命令とユーザ自身のAIDと任意のPATをSCS5に送信する。次に、SCS5は受信したAIDの署名を検証する。署名が正しくない場合には、SCS5は処理を終了する。署名が正しい場合には、SCS5は受信したすべてのPATについて、それぞれADSの公開鍵を用いて署名を検証する。署名が正しくないPATについては廃棄する。署名が正しい場合には、受信したAIDからリンク情報を取り出し、取り出したリンク情報をそれぞれのPATに提示して検索する。受信したAIDのリンク情報と完全一致するリンク情報を含むPATについては、登録命令とPATを記憶装置に提示して、PATを記憶装置に登録する。受信したAIDのリンク情報と完全一致するリンク情報を含まないPATについては記憶装置に登録せずに廃棄する。なお、上記処理において、ユーザとSCS5間の通信を暗号化する場合もある。

【0405】着信拒否の実行：SCS5はPATを記憶装置に提示して検索する。提示したPATと完全一致するPATが記憶装置に登録されている場合には、メールを廃棄する。提示したPATと完全一致するPATが記憶装置に登録されていない場合には、メールを廃棄しない。

【0406】着信拒否の解除：ユーザとセキュア・コミュニケーション・サービスSCS5との間で、任意の手段で双方向認証を行う。次に、ユーザは自らのAIDをSCS5に提示する。次に、SCS5は受信したAIDの署名を検証する。署名が正しくない場合には、SCS5は処理を終了する。署名が正しい場合には、SCS5は提示されたAIDからリンク情報を取り出し、取り出したリンク情報を検索条件として記憶装置に提示して、提示されたリンク情報を含むすべてのPATを取得し、ユーザに提示する。次に、ユーザは提示されたすべてのPATを参照し、着信拒否を解除したいPATをすべて選択し、削除命令と併せてSCS5に送信する。削除命令と着信拒否を解除したいすべてのPATを受信したSCS5は、受信した削除命令及びすべてのPATを記憶装置に提示して、受信したすべてのPATを記憶装置から削除する。

【0407】なお、SCSにおけるリンク指定型1対N個別化アクセスチケットPATに対する着信拒否方法も、上記リンク指定型1対1個別化アクセスチケットに対する着信拒否方法と同様である。

【0408】次に、図38のフローチャートおよび図39を参照して、同一性の判定について説明する。

【0409】1．変数OID_Mの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する。また、変数OID_Vの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する（ステップS7911）。

【0410】2．処理対象のリンク情報付きAIDの集合から1個のリンク情報付きAIDを選択し、以下のビット演算を実行する（ステップS7913）。

【0411】(a) リンク情報付きAIDに含まれる位置情報をもとにして、変数AID_Mと変数AID_Vの値を決定する（ステップS7915）。ここで、

・AID_MはOIDの全長Lと等しい長さで、かつ、

－OID情報が定義されている位置の値は1である。

－OID情報が定義されていない位置の値は0である。

ビット列と定義する（図39）。

【0412】・AID_VはOIDの全長Lと等しい長さで、かつ、

－OID情報が定義されている位置の値はOID情報の実際の値である。

－OID情報が定義されていない位置の値は0である。

ビット列と定義する（図39）。

【0413】(b) OID_MとAID_MのAND演算を実行し、その結果を変数OVR_Mに代入する（ステップS7917）。

【0414】(c) OVR_MとAID_MのAND演算と、OVR_MとOID_MのAND演算を実行し、その演算結果を比較する（ステップS7919）。

【0415】・一致する場合OID_MとAID_MのOR演算を実行し、実行結果をOID_Mに代入する（ステップS7921）。また、OID_VとAID_VのOR演算を実行し、実行結果をOID_Mに代入する（ステップS7923）。

【0416】・一致しない場合、ステップS7925に進み、実行する。

【0417】(d) 処理対象のリンク情報付きAIDの集合から、次に処理するリンク情報付きAIDを抽出す

る。

【０４１８】・集合に少なくとも１個のリンク情報付きＡＩＤが含まれている場合、ステップＳ７９１３－Ｓ７９２３を実行する。

【０４１９】・集合にリンク情報付きＡＩＤが１個も含まれていない場合、ステップＳ７９２７に進む。

【０４２０】(e) OID_M およびOID_V の値を出力する（ステップＳ７９２７）。

【０４２１】最終的に得られたOID_M の値は、処理対象のリンク情報付きＡＩＤの集合から復元できたＯＩＤ情報のすべての位置を表している。また、最終的に得られたOID_V の値は、処理対象のリンク情報付きＡＩＤの集合から復元できたＯＩＤ情報のすべてを表している。つまり、OID_M とOID_V の値を用いると、(a) OID_V の値を検索条件とすると、確率的にではあるがＯＩＤを求めることができる。

【０４２２】(b) 上記検索の精度を、ＯＩＤ全長Ｌとの比OID_M ／Ｌで定量的に評価することができる。

【０４２３】上述したように、本実施形態では、ユーザ要求に基づいて、秘密性かつ信用性の高い第三者機関である認証局ＣＡ１において、氏名、電話番号、実Ｅメールアドレス等秘密性の高い個人情報を含む個人識別子ＯＩＤからこれらの個人情報を隠蔽したリンク情報付き役割識別子ＡＩＤを生成し、ユーザに交付する。このＡＩＤを用いて通信網及び通信網上で提供される各種サービスにおいてユーザを識別することにより、ユーザの匿名性保証と本人証明の両立が可能になる。つまり、ユーザは実名や電話番号やＥメールアドレスを相手に教えなくても、お互いに通信できるようになるし、後述のように、アノニマス・ディレクトリ・サービスＡＤＳ７を介して不特定多数に公開情報を開示することもできる。

【０４２４】ユーザは、個人情報に比べ秘密性のより低いと思われる情報すなわち公開情報をアノニマス・ディレクトリ・サービスＡＤＳ７に登録する。公開情報及び登録者ＡＩＤを検索する場合には、検索者は検索者のリンク情報付き役割識別子ＡＩＤと任意の検索条件をアノニマス・ディレクトリ・サービスＡＤＳ７に提示する。アノニマス・ディレクトリ・サービスＡＤＳ７は、すべての検索条件を満足する登録者のリンク情報付き役割識別子ＡＩＤを抽出し、次に、検索者のリンク情報付き役割識別子ＡＩＤのリンク情報と検索条件を満足した登録者のリンク情報付き役割識別子ＡＩＤのリンク情報と移転制御フラグの値と有効期限の値からリンク指定型１対１個別化アクセスチケットＰＡＴを生成する。

【０４２５】このリンク指定型１対１個別化アクセスチケットＰＡＴには、図３４（ｃ）に示すように、移転制御フラグの値、有効期限の値が設定されるが、この有効期限を事前に設定することにより、発信者からの接続を制限することができる。

【０４２６】また、移転制御フラグの値により、アクセス権を有していない第三者からの接続を禁止することができる。すなわち、移転制御フラグを１に設定した場合には、セキュア・コミュニケーション・サービスＳＣＳ５と発信者との間で任意のチャレンジ／レスポンス方式に従い発信者役割識別子ＡＩＤを認証するため、発信者が発信者ＡＩＤとＰＡＴの両者を発信者以外のいかなるユーザに渡しても、そのユーザはアノニマス・ディレクトリ・サービスＡＤＳ７への登録者にＳＣＳ５を介して接続できない。一方、移転制御フラグを０に設定した場合には、ＳＣＳ５と発信者との間でいかなるチャレンジ／レスポンスも行わないため、発信者が発信者ＡＩＤとＰＡＴの両者を発信者以外のユーザに渡したら、それらのユーザもＡＤＳ７への登録者にＳＣＳ５を介して接続できるようになる。

【０４２７】また、リンク指定型１対１個別化アクセスチケットＰＡＴで着信者を指定した呼をリンク指定型１対１個別化アクセスチケットＰＡＴのリンク情報で特定した着信者役割識別子ＡＩＤまたは発信者役割識別子ＡＩＤに着信するように、通信網に対して接続要求をすることができる。更に、リンク指定型１対１個別化アクセスチケットＰＡＴで指定した呼のうち、着信者が選択したリンク指定型１対１個別化アクセスチケットＰＡＴの呼を着信拒否することができる。また、着信者が選択したリンク指定型１対１個別化アクセスチケットの呼の着信拒否を解除することもできる。更に、匿名性を悪用し複数の発信者役割識別子ＡＩＤで個人攻撃を繰り返す発信者への対処として、それら複数の発信者役割識別子ＡＩＤから個人識別子ＯＩＤの同一性を判定することができ、かつ、その個人識別子をある確率で取り出すことができる。

【０４２８】次に、本発明の第７の実施形態に係るメールアクセス制御方法について図４０乃至図４９を参照して説明する。上述した第６の実施形態では発信者と着信者を１対１に対応させる場合について説明したのに対して、第７の実施形態では、上述した第２の実施形態と同様に、発信者と着信者を１対Ｎに対応させるとともに、リンク指定型１対Ｎ個別化アクセスチケットの新規生成、内容変更をユーザ主導で可能とする場合について説明するものである。なお、この発信者はＰＡＴの所有者またはＰＡＴの会員のいづれかである。同様に受信者もＰＡＴの所有者またはＰＡＴの会員のいづれかである。

【０４２９】第２の実施形態で説明したと同様に、グループ通信（メーリングリスト等）の会員構成は動的に変化するため、グループ通信の主催者は会員の電話番号、電子メールアドレス等の連絡先情報を管理する必要がある。これに対して、第６の実施形態のように、リンク指定型１対１個別化アクセスチケットの新規生成しかできない場合には、連絡先情報の管理が困難である。例えば、グループを一体として管理することが困難であり、また移転制御のため、他の人に渡しても、メーリングリ

スト等グループ通信のアドレスとして機能しない。

【０４３０】本第７の実施形態では、このような不具合を解消するためにリンク指定型１対Ｎ個別化アクセスチケットＰＡＴの新規生成および既存のリンク指定型１対Ｎ個別化アクセスチケットＰＡＴの内容変更をユーザ主導でできるようにしている。

【０４３１】まず、本第７の実施形態で使用される各識別子の定義について図４０、図４１を参照して説明する。

【０４３２】個人識別子ＯＩＤは、図４０（ａ）に示すように、認証局ＣＡ１がユーザを一意に識別可能な規則に従う任意の文字列と公開鍵から構成される情報に対し認証局ＣＡ１が署名したものである。

【０４３３】リンク情報付き役割識別子ＡＩＤは、図４０（ｂ）に示すように、個人識別子ＯＩＤの断片とその位置情報、冗長な文字列、ＳＣＳを動かしているホストまたはドメインをネットワーク上で一意に識別可能な任意の文字列（ホスト名、実ドメイン名）であるＳＣＳの情報、およびリンク情報から構成される情報に対し認証局ＣＡ１が署名したものである。また、ＡＩＤはＳＣＳやＣＡで暗号化する場合もある。なお、リンク情報は、第６の実施形態のものと同じである。

【０４３４】リンク指定型１対Ｎ個別化アクセスチケット（Personalized Access Ticket：ＰＡＴ）は、図４０（ｃ）に示すように、２個以上の役割識別子のリンク情報、所有者インデックス、有効期限、移転制御フラグ、ＰＡＴ演算装置識別子から構成される情報に対し、ＰＡＴ演算装置の秘密鍵により署名したものである。

【０４３５】ここで、役割識別子ＡＩＤのリンク情報の１個は、このＰＡＴの所有者役割識別子ＡＩＤのリンク情報で、所有者ＡＩＤのリンク情報とこれに対応したEnabler をＰＡＴ演算装置に提示することにより、ＰＡＴへのＡＩＤのリンク情報の追加、ＰＡＴからのＡＩＤのリンク情報の削除、ＰＡＴの有効期限の変更、ＰＡＴの移転制御フラグの値の変更等、ＰＡＴに含まれる情報を変更することができる。

【０４３６】一方、ＰＡＴに含まれる所有者ＡＩＤのリンク情報以外のＡＩＤのリンク情報はすべて会員ＡＩＤのリンク情報で、会員ＡＩＤのリンク情報とこれに対応したEnabler をＰＡＴ演算装置に提示しても、ＰＡＴに含まれる情報を変更することはできない。

【０４３７】所有者インデックスは、所有者ＡＩＤのリンク情報を識別するための数値データで、所有者ＡＩＤのリンク情報と会員ＡＩＤのリンク情報とから構成されるリンク指定型ＡＩＤリストにおける先頭のＡＩＤのリンク情報が所有者ＡＩＤのリンク情報の場合には１、先頭から２番目のＡＩＤのリンク情報が所有者ＡＩＤのリンク情報の場合には２、…、ｎ番目のＡＩＤのリンク情報が所有者ＡＩＤのリンク情報の場合にはｎであると定義する。

【０４３８】移転制御フラグは、リンク指定型１対１個別化アクセスチケットの場合と同様、０または１の値をとりうると定義する。

【０４３９】所有者ＡＩＤのリンク情報は、リンク指定型ＡＩＤリストにおける所有者インデックスの値の位置に書き込まれているＡＩＤのリンク情報であると定義する。会員ＡＩＤのリンク情報は、所有者ＡＩＤのリンク情報以外のすべてのＡＩＤのリンク情報と定義する。

【０４４０】有効期限はＰＡＴの使用回数、ＰＡＴが利用不可能になる絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になる絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になってから利用不可能になるまでの相対時間（寿命）のいずれか、または複数を組み合わせて定義する。ＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）の識別子は、ＰＡＴ演算装置のシリアルナンバー（またはＰＡＴ演算オブジェクトのネットワーク上の識別名）であると定義する。

【０４４１】ＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）の秘密鍵は、前記識別子に一意に対応すると定義する。

【０４４２】また、本第７の実施形態では、役割識別子ＡＩＤに対応した識別子として、Enabler を導入している。Enabler は、図４１に示すように、Enabler であることを一意に表す文字列とリンク情報付きＡＩＤから構成される情報に対して認証局ＣＡ１が署名したものである。

【０４４３】次にＰＡＴの新規生成および内容変更における操作について説明する。通信端末上のセキュアなＰＡＴ演算装置、ＣＡ上もしくはＣＡから正当に依頼されたネットワーク上のＰＡＴ演算オブジェクト（以後、これもＰＡＴ演算装置と呼ぶことにする）において、次の操作が定義されるが、これは第２の実施形態のものと同じであり、図１０～図１３を参照して説明する。

【０４４４】１．リンク指定型ＡＩＤリストの編集

リンク情報付きＡＩＤとEnabler を用いて、ＰＡＴに含まれるＡＩＤのリンク情報のリストであるリンク指定型ＡＩＤリストを編集する。または、リンク指定型ＡＩＤリストを新規生成する。

【０４４５】２．有効期限及び移転制御フラグの値の設定

リンク情報付きＡＩＤとEnabler を用いて、ＰＡＴに含まれる有効期限の値および移転制御フラグの値を変更する。または、新たに生成したリンク指定型ＡＩＤリストに新たな有効期限の値及び新たな移転制御フラグの値を設定する。

【０４４６】所有者ＡＩＤとこの所有者ＡＩＤに対応したEnablerをＰＡＴ演算装置に提示したユーザは、ＰＡＴに含まれるＡＩＤのリンク情報のリストを編集できる。このとき、以下の演算規則に従う。

【０４４７】(1) 新規生成（MakeＰＡＴ）（図１０参

照）：
リンク指定型ＡＩＤリスト（ＬＡＬＩＳＴ＜（リンク）所有者ＡＩＤ｜（リンク）会員AID_1，（リンク）会員AID_2，…，（リンク）会員AID_n＞）（但し、（リンク）AID_X はAID_X のリンク情報であること

（リンク）AID_A ＋（リンク）AID_B
＋ Enabler of AID_B ＋ Enabler of AID_A
→ ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_B ＞
ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_B ＞
＋ Enabler of AID_A ＋ 有効期限の値 ＋ 移転制御フラグの値
→ ＰＡＴ＜（リンク）AID_A ｜（リンク）AID_B ＞

を表す）を新規生成し、生成後のＬＡＬＩＳＴに対し、有効期限の値および移転制御フラグの値を設定する。
【０４４８】
【数２３】

(2) マージ（MergePAT）（図１１参照）：
同一所有者ＡＩＤの複数ＬＡＬＩＳＴをマージし、マージ後のＬＡＬＩＳＴに対し、有効期限の値および移転制

ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_{B1}，（リンク）AID_{B2}，…＞
＋ ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_{C1}，（リンク）AID_{C2}，…＞
＋ Enabler of AID_A
→ ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_{B1}，（リンク）AID_{B2}，…，（リンク）AID_{C1}，（リンク）AID_{C2}，…＞
ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_{B1}，（リンク）AID_{B2}，…，（リンク）AID_{C1}，（リンク）AID_{C2}，…＞
＋ Enabler of AID_A ＋ 有効期限の値 ＋ 移転制御フラグの値
→ ＰＡＴ＜（リンク）AID_A ｜（リンク）AID_{B1}，（リンク）AID_{B2}，…，（リンク）AID_{C1}，（リンク）AID_{C2}，…＞

御フラグの値を設定する。
【０４４９】
【数２４】

(3) 分割（SplitＰＡＴ）（図１２参照）：
ＬＡＬＩＳＴを同一所有者ＡＩＤの複数ＬＡＬＩＳＴに分解し、分解後のすべてのＬＡＬＩＳＴに対し、それぞれ、有効期限の値および移転制御フラグの値を設定す

ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_{B1}，（リンク）AID_{B2}，…，（リンク）AID_{C1}，（リンク）AID_{C2}，…＞
＋ Enabler of AID_A
→ ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_{B1}，（リンク）AID_{B2}，…＞
＋ ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_{C1}，（リンク）AID_{C2}，…＞
ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_{C1}，（リンク）AID_{C2}，…＞
＋ Enabler of AID_A ＋ 有効期限の値 ＋ 移転制御フラグの値
→ ＰＡＴ＜（リンク）AID_A ｜（リンク）AID_{C1}，（リンク）AID_{C2}，…＞

る。
【０４５０】
【数２５】

(4) 所有者変更（TransＰＡＴ）（図１３参照）：
ＬＡＬＩＳＴの所有者ＡＩＤを変更し、変更後のＬＡＬＩＳＴに対し有効期限の値および移転制御フラグの値を

ＬＡＬＩＳＴ＜（リンク）AID_A ｜（リンク）AID_B ＞

設定する。
【０４５１】
【数２６】

+ LALIST<(リンク)AID_A | (リンク)AID_{C1},
(リンク)AID_{C2}, …>
+ Enabler of AID_A + Enabler of AID_B
→ LALIST<(リンク)AID_B | (リンク)AID_{C1},
(リンク)AID_{C2}, …>
LALIST<(リンク)AID_B | (リンク)AID_{C1},
(リンク)AID_{C2}, …>
+ Enabler of AID_B + 有効期限の値 + 移転制御フラグの値
→ PAT<(リンク)AID_B | (リンク)AID_{C1},
(リンク)AID_{C2}, …>

有効期限の値の設定における操作では、所有者ＡＩＤとこれに対応したEnabler の両者を所有するユーザにのみ有効期限の値の設定を許可するために、以下の操作を定義する。

【0452】

【数27】

PAT<(リンク)AID_A | (リンク)AID_B >
+ Enabler of AID_A + 有効期限の値
→ PAT<(リンク)AID_A | (リンク)AID_B >

移転制御フラグの値の設定における操作では、所有者ＡＩＤとこれに対応したEnabler の両者を所有するユーザにのみ移転制御フラグの値の設定を許可するために、以下の操作を定義する。

【0453】

【数28】

PAT<(リンク)AID_A | (リンク)AID_B >
+ Enabler of AID_A + 移転制御フラグの値
→ PAT<(リンク)AID_A | (リンク)AID_B >

次に、本実施形態の全体構成を示す図４２～図４８について説明する。図４２～図４８において、ＣＡからＡＩＤ$_A$ を割り当てられたユーザＡは、ユーザＡの計算機にＡＩＤ$_A$ および Enabler of ＡＩＤ$_A$ を保存し、フロッピードライブ、ＣＤ－ＲＯＭドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、記憶装置及びデータ入出力機能を備える通信端末（電話、携帯電話等）に、ＡＩＤ$_A$ および Enabler of ＡＩＤ$_A$ を保存している。

【0454】同様に、ＣＡからＡＩＤ$_B$ を割り当てられたユーザＢは、自らの計算機にＡＩＤ$_B$ および Enabler of ＡＩＤ$_B$ を保存し、フロッピードライブ、ＣＤ－ＲＯＭドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、記憶装置及びデータ入出力機能を備える通信端末（電話、携帯電話等）に、ＡＩＤ$_B$ および Enabler of ＡＩＤ$_B$ を保存している。

【0455】以下、ユーザＡがＰＡＴ<（リンク）ＡＩＤ$_A$ |（リンク）ＡＩＤ$_B$ >を生成する手順を説明する。

【0456】(1) ユーザＡは、以下の手段のいずれかを用いて、ＡＩＤ$_B$ および Enabler of ＡＩＤ$_B$ を取得する。

【0457】・アノニマス・ディレクトリ・サービスＡＤＳ７にＡＩＤ$_B$ と Enabler of ＡＩＤ$_B$ を登録し、ユーザＡが検索結果として取得するのを待つ（図４２）。

【0458】・電子メール、シグナリング等でＡＩＤ$_B$ と Enabler of ＡＩＤ$_B$ をユーザＡに直接送信する（図４３～図４４）。

【0459】・フロッピーディスク、ＣＤ－ＲＯＭ、ＭＯ、ＩＣカード等の磁気、光、電子メディアにＡＩＤ$_B$ と Enabler of ＡＩＤ$_B$ を蓄積し、ユーザＡに渡す。または、ユーザＡが閲覧して取得するのを待つ（図４５～図４６）。

【0460】・書籍、名刺等の紙メディアにＡＩＤ$_B$ と Enabler of ＡＩＤ$_B$ を記載し、ユーザＡに渡す。もしくは、ユーザＡが閲覧し取得するのを待つ（図４７～図４８）。

【0461】(2) 上述した（１）のいずれかの手段でＡＩＤ$_B$ および Enabler of ＡＩＤ$_B$ を取得したユーザＡは、ＰＡＴ演算装置に対しMakeＰＡＴ命令を発行する。この手順は図４２～図４８で共通で、以下の通りに定義する。

【0462】(a) ユーザＡは、ユーザＡの通信端末にＡＩＤ$_A$ 、Enabler of ＡＩＤ$_A$ 、ＡＩＤ$_B$ 、Enabler of ＡＩＤ$_B$ 、有効期限の値、および移転制御フラグの値をセットし、MakeＰＡＴ命令の発行を要求する。

【0463】(b) ユーザＡの通信端末は、MakeＰＡＴ命令を生成する。

【0464】(c) ユーザＡの通信端末は、生成したMakeＰＡＴ命令を電子メール、シグナリング等の手段でＰＡＴ演算装置に送信する（MakeＰＡＴ命令の発行）。

【0465】(d) ＰＡＴ演算装置は、受信したMakeＰＡＴ命令を図２１、図４９に従って処理し、ＰＡＴ<（リンク）ＡＩＤ$_A$ |（リンク）ＡＩＤ$_B$ >を生成する。具体的には、

【数29】

（リンク）AID_A ＋（リンク）AID_B
＋ Enabler of AID_B ＋ Enabler of AID_A
→ LALIST＜（リンク）AID_A ｜（リンク）AID_B ＞
LALIST＜（リンク）AID_A ｜（リンク）AID_B ＞
＋ Enabler of AID_A ＋ 有効期限の値 ＋ 移転制御フラグの値
→ PAT＜（リンク）AID_A ｜（リンク）AID_B ＞

(e) ＰＡＴ演算装置は、生成したＰＡＴ＜（リンク）AID_A ｜（リンク）AID_B ＞を電子メール、シグナリング等の手段でユーザＡの通信端末、または必要に応じて、ユーザＢの通信端末に送信する。

【０４６６】(f) ユーザＡ（またはユーザＢ）の通信端末は、受信したＰＡＴ＜（リンク）AID_A ｜（リンク）AID_B ＞をユーザＡの通信端末の記憶装置に保存する。

【０４６７】ＰＡＴのマージ（MergeＰＡＴ、図２１、図４９）、ＰＡＴの分割（SplitＰＡＴ、図２２、図４９）、ＰＡＴの所有者変更（TransＰＡＴ、図２１、図４９）も同様の手順である。

【０４６８】MakeＰＡＴ、MergeＰＡＴ、TransＰＡＴの手順については、ＡＩＤをＡＩＤのリンク情報に置き換えＡＩＤリストをリンク指定型ＡＩＤリストに置き換える以外は図２１を参照して前述した通りである。また、SplitＰＡＴの手順についても、ＡＩＤをＡＩＤのリンク情報に置き換えＡＩＤリストをリンク指定型ＡＩＤリストに置き換える以外は図２２を参照して前述したとおりである。

【０４６９】但し、図２１、図２２の手順において、リンク指定型ＡＩＤリストの生成は、図４９のフローチャートにより次のように行う。すなわち、まずバッファ長を決定し（ステップＳ９０１１）、バッファを生成する（ステップＳ９０１２）。次いで、所有者ＡＩＤのリンク情報を生成したバッファの空き領域にコピーする（ステップＳ９０１７）。次いで、会員ＡＩＤのリンク情報をバッファの空き領域にコピーし（ステップＳ９０１８）、次の会員ＡＩＤが存在すれば（ステップＳ９０１５ＹＥＳ）ステップＳ９０１８を繰り返す。

【０４７０】次に、所有者ＡＩＤのリンク情報の決定について説明する。

【０４７１】MakeＰＡＴ、MergeＰＡＴ、SplitＰＡＴ、TransＰＡＴの各命令は、２個以上の引数を持ち、引数として、役割識別子ＡＩＤ、個別化アクセスチケットＰＡＴ、または、Enabler を指定できると定義する。このとき、ＰＡＴ演算装置は、各命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報をそれぞれ下記の規則に従い指定する。

SplitＰＡＴ PAT_1 （AID_{11}）（AID_{21} AID_{22}）…
（AID_{N1} AID_{N2} … AID_{NM}） Enabler of ＡＩＤ

－ＰＡＴ演算装置は、SplitＰＡＴ命令の第１引数のＰＡＴの所有者ＡＩＤのリンク情報を、SplitＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報であると解釈する。

【０４７２】・MakeＰＡＴの場合

MakeＰＡＴ命令に対して、第１引数から第Ｎ引数（Ｎ＝２，３，…）までＡＩＤを、第Ｎ＋１引数以降ではEnabler を指定すると定義する。例えば、

MakeＰＡＴ AID_1 AID_2 … AID_N Enabler of AID_1
Enabler of AID_2 … Enabler of AID_N

－ＰＡＴ演算装置は、MakeＰＡＴ命令の第１引数のＡＩＤのリンク情報を所有者ＡＩＤのリンク情報であると解釈する。

【０４７３】－第Ｎ＋１引数以降のEnabler のいずれかが第１引数のＡＩＤに対応している場合に限り、ＰＡＴ演算装置はこのＡＩＤのリンク情報（すなわち、第１引数のＡＩＤのリンク情報）をMakeＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報に指定する。

【０４７４】・MergeＰＡＴの場合

MergeＰＡＴ命令に対して、第１引数から第Ｎ引数（Ｎ＝２，３，…）までＰＡＴを、第Ｎ＋１引数ではEnablerを指定すると定義する。すなわち、

MergeＰＡＴ PAT_1 PAT_2 … PAT_N Enabler of ＡＩＤ

－ＰＡＴ演算装置は、MergeＰＡＴ命令の第１引数のＰＡＴの所有者ＡＩＤのリンク情報を、MergeＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報であると解釈する。

【０４７５】－第Ｎ＋１引数のEnabler が第１引数のＰＡＴの所有者ＡＩＤに対応している場合に限り、ＰＡＴ演算装置はこのＡＩＤのリンク情報（すなわち、第１引数のＰＡＴの所有者ＡＩＤのリンク情報）をMergeＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報に指定する。

【０４７６】・SplitＰＡＴの場合

SplitＰＡＴ命令に対して、第１引数でＰＡＴを、第２引数から第Ｎ引数（Ｎ＝３，４，…）まではあらかじめ定められた何らかの記号（この例ではカッコ（）とする）でまとめられた１個以上のＡＩＤのまとまりを、第Ｎ＋１引数ではEnablerを指定すると定義する。すなわち、

SplitＰＡＴ PAT_1 （AID_{11}）（AID_{21} AID_{22}）…
（AID_{N1} AID_{N2} … AID_{NM}） Enabler of ＡＩＤ

実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報であると解釈する。

【0477】－第N＋1引数のEnabler が第1引数のＰＡＴの所有者ＡＩＤに対応している場合に限り、ＰＡＴ演算装置はこのＡＩＤのリンク情報（すなわち、第1引数のＰＡＴの所有者ＡＩＤのリンク情報）をSplitＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報に指定する。

・TransＰＡＴの場合

TransＰＡＴ命令に対して、第1引数及び第2引数でＰＡＴを、第3引数でＡＩＤを、第4引数及び第5引数ではEnablerを指定すると定義する。すなわち、

TransＰＡＴ　PAT_1 PAT_2 ＡＩＤ

Enabler of AID_1 Enabler of AID_2

－ＰＡＴ演算装置は、TransＰＡＴ命令の第3引数のＡＩＤのリンク情報が第2引数のＰＡＴに含まれている場合に限り、第3引数のＡＩＤのリンク情報を、TransＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報であると解釈する。

【0479】－第4引数のEnabler が第1引数のＰＡＴ及び第2引数のＰＡＴの両者に対応しており、かつ、第5引数のEnabler が第3引数のＡＩＤに対応している場合に限り、ＰＡＴ演算装置は第3引数のＡＩＤのリンク情報をTransＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報に指定する。

【0480】次に、会員ＡＩＤのリンク情報の決定について説明する。MakeＰＡＴ，MergeＰＡＴ，SplitＰＡＴ，TransＰＡＴ各命令の定義は上記に従う。ＰＡＴ演算装置は、各命令実行後に出力されるＰＡＴの会員ＡＩＤのリンク情報をそれぞれ下記の規則に従い指定する。

【0481】・MakeＰＡＴの場合

MakeＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報が正式に決定された場合に限り、

－ＰＡＴ演算装置は、MakeＰＡＴ命令の第2引数以降のすべてのＡＩＤのリンク情報をMakeＰＡＴ命令実行後に出力されるＰＡＴの会員ＡＩＤのリンク情報であると解釈する。

SplitＰＡＴ　ＰＡＴ（AID_{11}）（AID_{21} AID_{22}）…（AID_{N1} AID_{N2} … AID_{NM}） Enabler of ＡＩＤ

の場合、（AID_{11}）と（AID_{21} AID_{22}）と（AID_{N1} AID_{N2} … AID_{NM}）のリンク情報は所有者ＡＩＤのリンク情報が共通な別のＰＡＴの会員ＡＩＤのリンク情報になる。

【0485】・TransＰＡＴの場合

ＰＡＴ演算装置は、TransＰＡＴ命令実行後に出力されるＰＡＴの所有者ＡＩＤのリンク情報が正式に決定された場合に限り、TransＰＡＴ命令の第1引数で指定されたＰＡＴのすべての会員ＡＩＤのリンク情報及び第2引数で指定されたＰＡＴの会員ＡＩＤのリンク情報のうち新所有者となる予定の会員ＡＩＤのリンク情報を除いた残りのすべての会員ＡＩＤのリンク情報を、TransＰＡＴ命令実行後に出力されるＰＡＴの会員ＡＩＤのリンク情報に指定する。

【0486】本実施形態の、Enabler の正当性の検証は図24を参照した前述した説明と同じである。また、このEnabler の正当性の検証は、MakeＰＡＴ、MergeＰＡＴ、SplitＰＡＴ、TransＰＡＴで共通である。

【0487】次に、本発明の第8の実施形態について説明する。

【0488】本第8の実施形態においては、個人識別子ＯＩＤは実メールアドレスである。個別化アクセスチケットＰＡＴは2個以上の実メールアドレス、所有者インデックス、有効期限、移転制御フラグ、及び、ＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）の識別子から構成される情報に対して、ＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）の秘密鍵で署名したものである。

【0489】実メールアドレスのうち、1個はこのＰＡＴの所有者メールアドレスで、所有者メールアドレスと所有者メールアドレスを含むEnabler の両者をＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）に提示することにより、ＰＡＴへの実メールアドレスの追加、削除、ＰＡＴの有効期限の変更、ＰＡＴの移転制御フラグの値の変更など、ＰＡＴに含まれる情報を変更することができる。

【0490】一方、ＰＡＴに含まれる実メールアドレスのうち、所有者メールアドレス以外の実メールアドレス

はすべて会員メールアドレスで、会員メールアドレスと会員メールアドレスを含むEnabler をＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）に提示しても、ＰＡＴに含まれる情報を変更することはできない。

【０４９１】所有者インデックスは、所有者メールアドレスを識別するための数値データである。所有者メールアドレスと会員メールアドレスから構成されるメールアドレスリストにおいて、先頭の実メールアドレスが所有者メールアドレスの場合には１、先頭から２番目の場合には２、…、ｎ番目の場合にはｎであると定義する。

【０４９２】メールアドレスリストにおいて、所有者メールアドレスは所有者インデックスで指定された位置に書き込まれている実メールアドレスと定義する。一方、会員メールアドレスは、所有者メールアドレス以外のすべての実メールアドレスであると定義する。

【０４９３】移転制御フラグは０または１の値をとりうると定義する。

【０４９４】有効期限はＰＡＴの使用回数、ＰＡＴが利用不可能になる絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になる絶対時刻（ＵＴＣ）、ＰＡＴが利用可能になってから利用不可能になるまでの相対時間（寿命）のいずれか、または複数を組み合わせて定義する。

【０４９５】ＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）の識別子は、ＰＡＴ演算装置のシリアルナンバー（またはＰＡＴ演算オブジェクトのネットワーク上の識別名）であると定義する。

【０４９６】ＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）の秘密鍵は、前記識別子に一意に対応すると定義する。

【０４９７】また、実メールアドレスに対応した識別子として、Enablerを定義する。Enablerは、Enablerであることを一意にあらわす情報と実メールアドレスから構成されるデータに対して、ＰＡＴ演算装置（またはネットワーク上のＰＡＴ演算オブジェクト）の秘密鍵で署名したものである。

【０４９８】ＰＡＴの生成は以下のように行う。

【０４９９】ネットワーク上のＰＡＴ演算オブジェクトの一例として、ディレクトリを挙げる。ディレクトリはユーザの実メールアドレスと公開情報を対応づけて管理し、任意のユーザから提示された検索条件を入力し、ＰＡＴを出力する。

【０５００】ユーザは実メールアドレスと検索条件をディレクトリに送信する。ディレクトリは検索条件を満足する公開情報と一意に対応した実メールアドレスをすべて取得する。次に、検索条件を提示したユーザの実メールアドレスと、検索結果として取得したすべての実メールアドレスから実メールアドレスのリストを構成する。次に、所有者インデックスの値、有効期限の値、転移制御フラグの値、及び、ディレクトリの識別名を追加する。最後に、これらをすべて追加したデータに対しディレクトリの秘密鍵で署名してＰＡＴとして、検索条件を提示したユーザに送信する。

【０５０１】メールアクセス制御は以下のように行う。

【０５０２】発信者はメールのＦｒｏｍ：行に送信者の実メールアドレスを、Ｔｏ：行にＰＡＴ@発信者の実ドメインを指定する。

【０５０３】ＳＣＳはＳＭＴＰ(Simple Mail Transfer Protocol)等のＭＴＡ(Message Transfer Agent)への着信メールを取得し、以下の手順に従い認証する。

【０５０４】１．ＰＡＴの署名をＰＡＴの公開鍵を用いて検証する。

【０５０５】・ＰＡＴに改竄が認められる場合には、メールを廃棄して終了する。

【０５０６】・ＰＡＴに改竄が認められない場合には、下記処理２．を実行する。

【０５０７】２．発信者の実メールアドレスをＰＡＴに提示して検索する。

【０５０８】・発信者の実メールアドレスと完全一致する実メールアドレスがＰＡＴに含まれていない場合には、メールを廃棄して終了する。

【０５０９】・発信者の実メールアドレスと完全一致する実メールアドレスがＰＡＴに含まれている場合には、下記処理３．を実行する。

【０５１０】３．ＰＡＴの有効期限を評価する。

【０５１１】・ＰＡＴが有効期限外の場合には、メールを廃棄して終了する。

【０５１２】・ＰＡＴが有効期限内の場合には、下記処理４．を実行する。

【０５１３】４．ＰＡＴの移転制御フラグの値を参照して、発信者を認証するか否かを決定する。

【０５１４】・値が１の場合には、ＳＣＳと発信者との間でチャレンジ／レスポンス認証を実行して、発信者の署名を検証する。署名が正しい場合には、着信者を指定し、ＰＡＴを添付する。署名が正しくない場合には、メールを廃棄して終了する。

【０５１５】・値が０の場合には、チャレンジ／レスポンス認証を実行せずに、着信者を指定し、チケットを添付する。

【０５１６】ＳＣＳと発信者との間のチャレンジ／レスポンスの例を説明する。

【０５１７】まず、ＳＣＳは任意の情報、例えばタイムスタンプを生成し、生成した情報を発信者に任意の手段で送信する。

【０５１８】次に、発信者は秘密鍵と公開鍵を生成し、受信した情報に秘密鍵で署名し、公開鍵とあわせてＳＣＳに任意の手段で送信する。

【０５１９】最後に、ＳＣＳは、受信した情報の署名を発信者から提示された公開鍵を用いて検証する。署名が正しい場合には、着信者を指定し、ＰＡＴを添付する。

署名が正しくない場合にはメールを廃棄して終了する。
【０５２０】着信者の指定及びチケットの添付は以下のように行う。
【０５２１】ＳＣＳは、まず、発信者の実メールアドレスをＰＡＴに提示して検索し、発信者の実メールアドレスと完全一致しないすべての実メールアドレスを取得する。次に、取得したすべての実メールアドレスを着信者の実メールアドレスに指定する。
【０５２２】次に、ＳＣＳは、双方向通信を可能とすべく、ＰＡＴをすべて着信者メールアドレスに送信するために、ＰＡＴをメールの任意の箇所に添付する。
【０５２３】最後に、ＳＣＳはＭＴＡにメールを渡す。
【０５２４】着信拒否は以下のように行う。
【０５２５】着信拒否の設定：ユーザとセキュア・コミュニケーション・サービスＳＣＳ５との間で、任意の手段で双方向認証を行う。次に、ユーザは登録命令とユーザ自身の実メールアドレスと任意のＰＡＴをＳＣＳ５に送信する。次に、ＳＣＳ５は受信したすべてのＰＡＴについて、それぞれＡＤＳの公開鍵を用いて署名を検証する。署名が正しくないＰＡＴについては廃棄する。署名が正しい場合には、受信した実メールアドレスをそれぞれのＰＡＴに提示して検索する。受信した実メールアドレスと完全一致する実メールアドレスを含むＰＡＴについては、登録命令とＰＡＴを記憶装置に提示して、ＰＡＴを記憶装置に登録する。受信した実メールアドレスと完全一致する実メールアドレスを含まないＰＡＴについては記憶装置に登録せずに廃棄する。
【０５２６】着信拒否の実行：ＳＣＳ５はＰＡＴを記憶装置に提示して検索する。提示したＰＡＴと完全一致するＰＡＴが記憶装置に登録されている場合には、メールを廃棄する。提示したＰＡＴと完全一致するＰＡＴが記憶装置に登録されていない場合には、メールを廃棄しない。
【０５２７】着信拒否の解除：ユーザとセキュア・コミュニケーション・サービスＳＣＳ５との間で、任意の手段で双方向認証を行う。次に、ユーザは自らの実メールアドレスをＳＣＳ５に提示する。次に、ＳＣＳ５は提示された実メールアドレスを検索条件として記憶装置に提示して、提示された実メールアドレスを含むすべてのＰＡＴを取得し、ユーザに提示する。次に、ユーザは提示されたすべてのＰＡＴを参照し、着信拒否を解除したいＰＡＴをすべて選択し、削除命令と併せてＳＣＳ５に送信する。削除命令と着信拒否を解除したいすべてのＰＡＴを受信したＳＣＳ５は、受信した削除命令及びすべてのＰＡＴを記憶装置に提示して、受信したすべてのＰＡＴを記憶装置から削除する。
【０５２８】ＰＡＴの編集は以下のように行う。
【０５２９】役割識別子ＡＩＤを要素とするＰＡＴに対するMakeＰＡＴ、MergeＰＡＴ、SplitＰＡＴ、TransＰＡＴ演算において、役割識別子ＡＩＤを実メールアドレスに、役割識別子ＡＩＤに対するEnabler を実メールアドレスに対するEnabler にそれぞれ置き換えると、実メールアドレスを要素とするＰＡＴに対するMakeＰＡＴ、MergeＰＡＴ、SplitＰＡＴ、TransＰＡＴ演算になる。
【０５３０】Ｎｕｌｌ演算子はＮｕｌｌであることを一意に表し、かつ、実メールアドレスの形式を持つ情報から構成される情報に対し、ＰＡＴ演算装置またはネットワーク上のＰＡＴ演算オブジェクトの秘密鍵で署名したものである。
【０５３１】同様に、Ｇｏｄ演算子はＧｏｄであることを一意に表し、かつ、実メールアドレスの形式を持つ情報から構成される情報に対し、ＰＡＴ演算装置またはネットワーク上のＰＡＴ演算オブジェクトの秘密鍵で署名したものである。
【０５３２】Ｎｕｌｌ演算子のEnabler はEnabler であることを一意に表す情報とＮｕｌｌ演算子の実体から構成される情報に対し、ＰＡＴ演算装置またはネットワーク上のＰＡＴ演算オブジェクトの秘密鍵で署名したものである。
【０５３３】Ｎｕｌｌ演算子及びはＧｏｄ演算子を用いた演算は、役割識別子ＡＩＤを要素とするＰＡＴに対するすべての演算において、役割識別子ＡＩＤを実メールアドレスに、役割識別子ＡＩＤに対するEnabler を実メールアドレスに対するEnabler に置き換えることで求められる。さらに、Ｎｕｌｌ−ＡＩＤをＮｕｌｌ演算子に、Ｇｏｄ−ＡＩＤをＧｏｄ演算子に、また、Ｎｕｌｌ−ＡＩＤに対するEnabler をＮｕｌｌ演算子に対するEnabler に置き換えることで求められる。
【０５３４】
【発明の効果】以上説明したように、本発明によれば、個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間のメールアクセス制御を行うので、ユーザの本当の識別子を隠蔽しつつ、ユーザの特性を表す情報を公開し、この情報に基づいて適切な通信を行うことができ、第三者からの攻撃等を防止することができる。加えて、着信者が匿名性を悪用した発信者による攻撃を受けた場合には、その攻撃による着信者への被害を最小限に食い止めることができる。
【０５３５】また、本発明によれば、個別化アクセスチケットの新規生成、内容変更を各ユーザに付与された役割識別子ＡＩＤとこのＡＩＤに対応して定義されたEnablerを用いてユーザ主導で行うことができるので、例えば動的に変化するグループ通信（メーリングリスト等）の会員の連絡先情報等も適確に管理することができる。
【０５３６】更に、本発明によれば、Ｎｕｌｌ−ＡＩＤとＮｕｌｌ−ＡＩＤの Enablerを導入して、会員ＡＩＤおよび Enabler of 会員ＡＩＤを個別化アクセスチケットＰＡＴの所有者に渡さなくてもＰＡＴの新規生成（MakeＰＡＴ）および所有者変更（TransＰＡＴ）を行うことができるので、会員ＡＩＤを用いた成りすましを防止

することができる。

【0537】本発明によれば、Null-AIDは個別化アクセスチケットPATの所有者AIDとしてのみ使用可能（Null-AIDはPATの会員AIDには使用不可能）であり、PAT<AID_{Null}|$AID_{member1}$, $AID_{member2}$, …, $AID_{memberN}$>は許可するがPAT<AID_{holder}|AID_{Null}, $AID_{member1}$, $AID_{member2}$, …, $AID_{memberN}$>は許可しないので、PAT<AID_{holder}|AID_{member}>の所有者がAID_{member}のEnabler を知らない限り、このPAT<AID_{holder}|AID_{member}>からPAT<AID_{Null}|AID_{member}>を作成することはできない。

【0538】また、本発明によれば、God-AIDを導入して、個別化アクセスチケットPATに読取専用属性を設定できるので、グループ通信において参加者を固定することができる。

【0539】更に、本発明によれば、役割識別子を一意に特定するためのリンク情報を導入して、個別化アクセスチケットPATをリンク情報により定義してPATには役割識別子の実体を含まないようにできるため、役割識別子の実体を使用することなく着信拒否機能を実現することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態の全体構成図。

【図2】第1の実施形態に使用される個人識別子OIDと役割識別子AIDと個別化アクセスチケットPATのデータ構造を示す図。

【図3】第1の実施形態での認証局CAにおける役割識別子AIDの生成処理を示すフローチャート。

【図4】第1の実施形態でのアノニマス・ディレクトリ・サービスADSにおける個別化アクセスチケットPATの生成処理を示すフローチャート。

【図5】第1の実施形態でのセキュア・コミュニケーション・サービスSCSにおけるメール転送制御を示すフローチャート。

【図6】第1の実施形態でのセキュア・コミュニケーション・サービスSCSにおける役割識別子AIDの同一性判定処理を示すフローチャート。

【図7】図6に示す同一性判定処理に用いるデータの例を示す図。

【図8】本発明の第2の実施形態に使用される個人識別子OIDと役割識別子AIDと個別化アクセスチケットPATのデータ構造を示す図。

【図9】本発明の第2の実施形態に使用される役割識別子AIDとEnabler のデータ構造を示す図。

【図10】本発明の第2の実施形態に使用される演算規則（MakePAT）の定義を示す図。

【図11】本発明の第2の実施形態に使用される演算規則（MergePAT）の定義を示す図。

【図12】本発明の第2の実施形態に使用される演算規則（SplitPAT）の定義を示す図。

【図13】本発明の第2の実施形態に使用される演算規則（TransPAT）の定義を示す図。

【図14】本発明の第2の実施形態におけるシステム構成（1）を示す図。

【図15】本発明の第2の実施形態におけるシステム構成（2）を示す図。

【図16】本発明の第2の実施形態におけるシステム構成（3）を示す図。

【図17】本発明の第2の実施形態におけるシステム構成（4）を示す図。

【図18】本発明の第2の実施形態におけるシステム構成（5）を示す図。

【図19】本発明の第2の実施形態におけるシステム構成（6）を示す図。

【図20】本発明の第2の実施形態におけるシステム構成（7）を示す図。

【図21】本発明の第2の実施形態での演算処理（MakePAT, MergePAT, TransPAT）の流れを示すフローチャート。

【図22】本発明の第2の実施形態での演算処理（SplitPAT）の流れを示すフローチャート。

【図23】本発明の第2の実施形態におけるAIDリストの生成処理（MakePAT, MergePAT, SplitPAT, TransPAT）を示すフローチャート。

【図24】本発明の第2の実施形態におけるEnabler の正当性の検証処理（MakePAT, MergePAT, SplitPAT, TransPAT）を示すフローチャート。

【図25】本発明の第3の実施形態に使用されるNull-AIDのデータ構造を示す図。

【図26】本発明の第3の実施形態に使用される Enabler of Null-AIDのデータ構造を示す図。

【図27】本発明の第3の実施形態の第1の応用例を示す図。

【図28】本発明の第3の実施形態の第2の応用例を示す図。

【図29】本発明の第4の実施形態に使用されるGod-AIDのデータ構造を示す図。

【図30】本発明の第4の実施形態の第1の応用例を示す図。

【図31】本発明の第4の実施形態の第2の応用例を示す図。

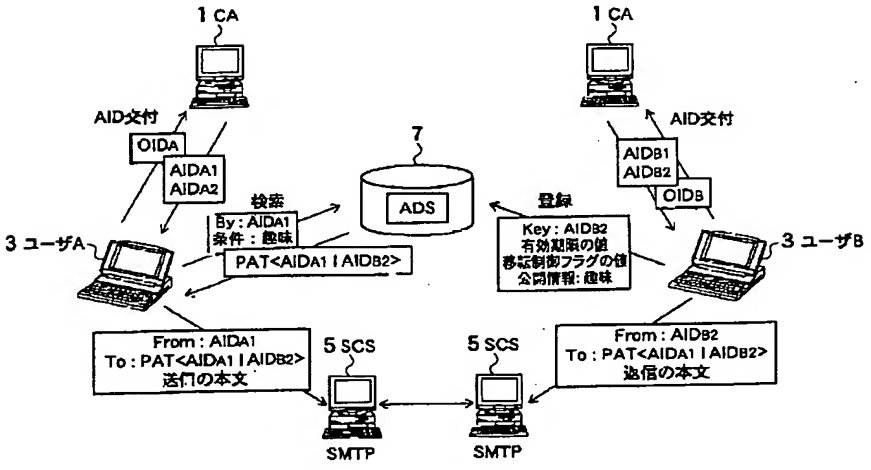
【図32】本発明の第5の実施形態における会員AIDのチェック処理を示すフローチャート。

【図33】本発明の第6の実施形態の全体構成図。

【図34】第6の実施形態に使用される個人識別子OID、リンク情報付き役割識別子AID、リンク指定型1対1個別化アクセスチケットPATのデータ構造を示す図。

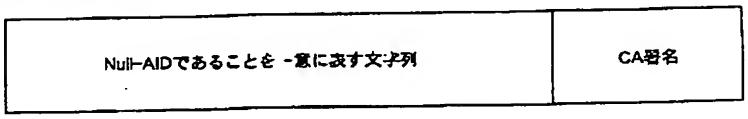
【図３５】第６の実施形態での認証局ＣＡにおけるリンク情報付き役割識別子ＡＩＤの生成処理を示すフローチャート。
【図３６】第６の実施形態でのアノニマス・ディレクトリ・サービスＡＤＳにおけるリンク指定型１対１個別化アクセスチケットＰＡＴの生成処理を示すフローチャート。
【図３７】第６の実施形態でのセキュア・コミュニケーション・サービスＳＣＳにおけるメール転送制御を示すフローチャート。
【図３８】第６の実施形態でのセキュア・コミュニケーション・サービスＳＣＳにおけるリンク情報付き役割識別子ＡＩＤの同一性判定処理を示すフローチャート。
【図３９】図３８に示す同一性判定処理に用いるデータの例を示す図。
【図４０】本発明の第７の実施形態に使用される個人識別子ＯＩＤ、リンク情報付き役割識別子ＡＩＤ、リンク指定型１対Ｎ個別化アクセスチケットＰＡＴのデータ構造を示す図。
【図４１】本発明の第７の実施形態に使用されるリンク情報付き役割識別子ＡＩＤとEnabler のデータ構造を示す図。
【図４２】本発明の第７の実施形態におけるシステム構成（１）を示す図。
【図４３】本発明の第７の実施形態におけるシステム構成（２）を示す図。
【図４４】本発明の第７の実施形態におけるシステム構成（３）を示す図。
【図４５】本発明の第７の実施形態におけるシステム構成（４）を示す図。
【図４６】本発明の第７の実施形態におけるシステム構成（５）を示す図。
【図４７】本発明の第７の実施形態におけるシステム構成（６）を示す図。
【図４８】本発明の第７の実施形態におけるシステム構成（７）を示す図。
【図４９】本発明の第７の実施形態におけるリンク指定型ＡＩＤリストの生成処理（MakePAT，MergePAT，SplitPAT，TransPAT）を示すフローチャート。
【符号の説明】
1　認証局ＣＡ
3　ユーザ
5　セキュア・コミュニケーション・サービスＳＣＳ
7　アノニマス・ディレクトリ・サービスＡＤＳ

【図１】

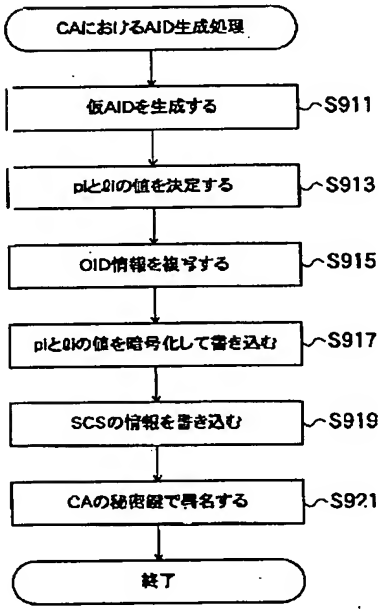


【図２５】

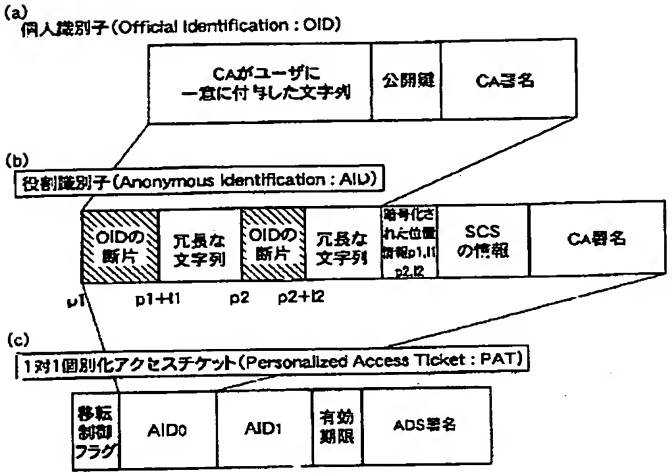
Null AIDのデータ構造



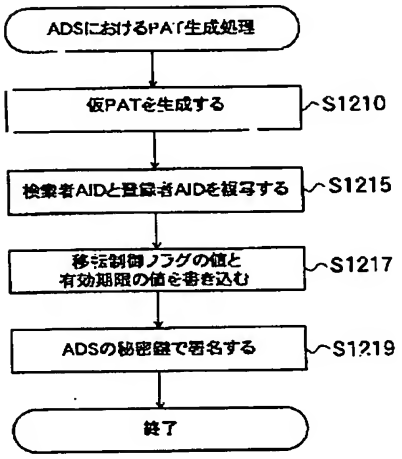
【図３】



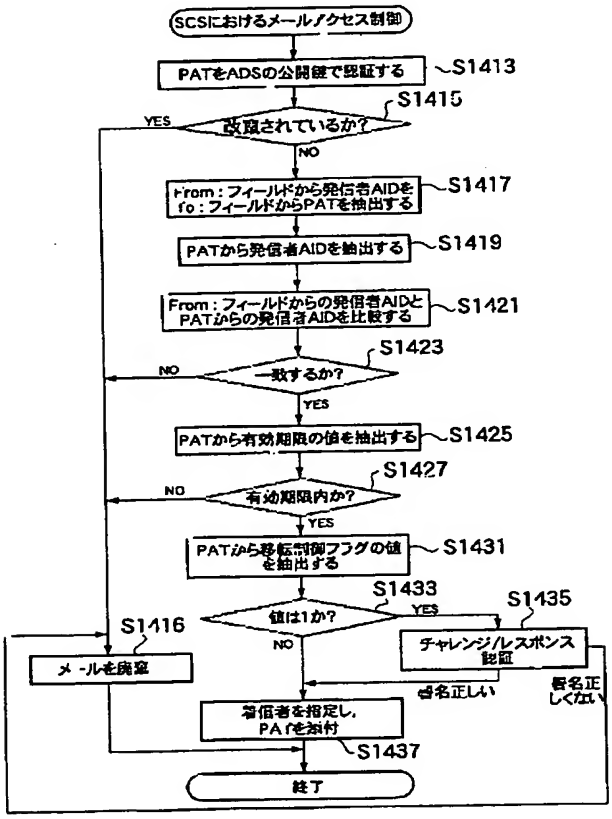
【図2】


(a)
個人識別子(Official Identification : OID)
CAがユーザに一意に付与した文字列
公開鍵
CA署名
(b)
役割識別子(Anonymous Identification : AID)
OIDの断片
冗長な文字列
OIDの断片
冗長な文字列
暗号化された位置情報p1,l1 p2,l2
SCSの情報
CA署名
p1
p1+l1
p2
p2+l2
(c)
1対1個別化アクセスチケット(Personalized Access Ticket : PAT)
移転制御フラグ
AID0
AID1
有効期限
ADS署名

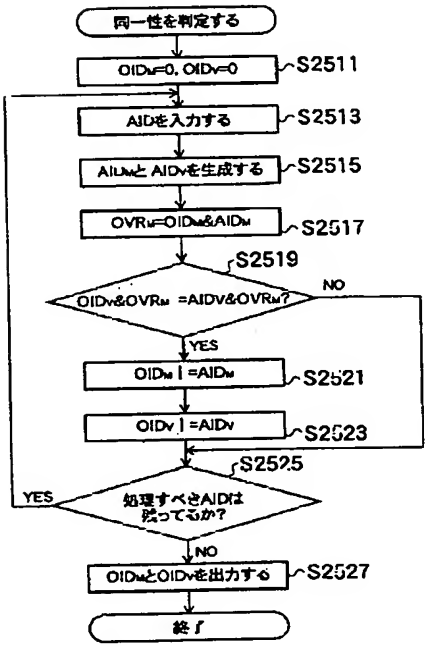
【図4】


ADSにおけるPAT生成処理
仮PATを生成する
S1210
検索者AIDと登録者AIDを複写する
S1215
移転制御フラグの値と有効期限の値を書き込む
S1217
ADSの秘密鍵で署名する
S1219
終了

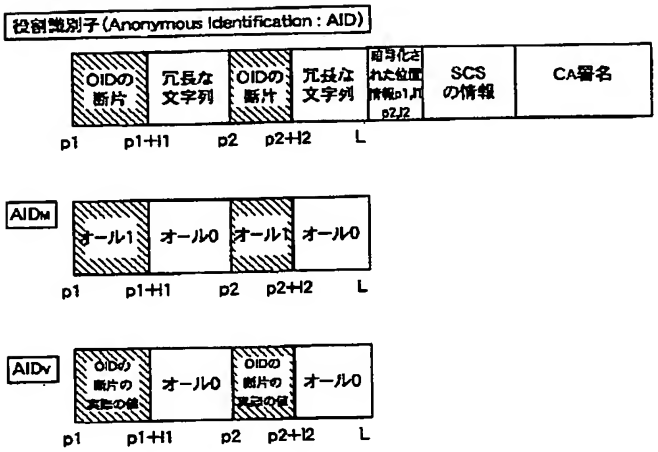
【図5】


SCSにおけるメールアクセス制御
PATをADSの公開鍵で認証する
S1413
改竄されているか?
S1415
YES
NO
From : フィールドから発信者AIDを抽出する
To : フィールドからPATを抽出する
S1417
PATから発信者AIDを抽出する
S1419
From : フィールドからの発信者AIDとPATからの発信者AIDを比較する
S1421
一致するか?
S1423
NO
YES
PATから有効期限の値を抽出する
S1425
有効期限内か?
S1427
NO
YES
PATから移転制御フラグの値を抽出する
S1431
値は1か?
S1433
YES
NO
S1435
チャレンジ/レスポンス認証
署名正しい
署名正しくない
メールを廃棄
S1416
着信者を指定し、PATを添付
S1437
終了

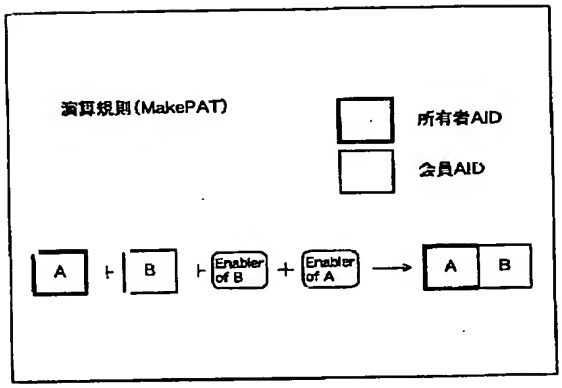
【図6】


同一性を判定する
OIDM=0, OIDV=0
S2511
AIDを入力する
S2513
AIDMとAIDVを生成する
S2515
OVRM=OIDM&AIDM
S2517
S2519
OIDV&OVRM =AIDV&OVRM?
NO
YES
OIDM | =AIDM
S2521
OIDV | =AIDV
S2523
S2525
処理すべきAIDは残ってるか?
YES
NO
OIDMとOIDVを出力する
S2527
終了

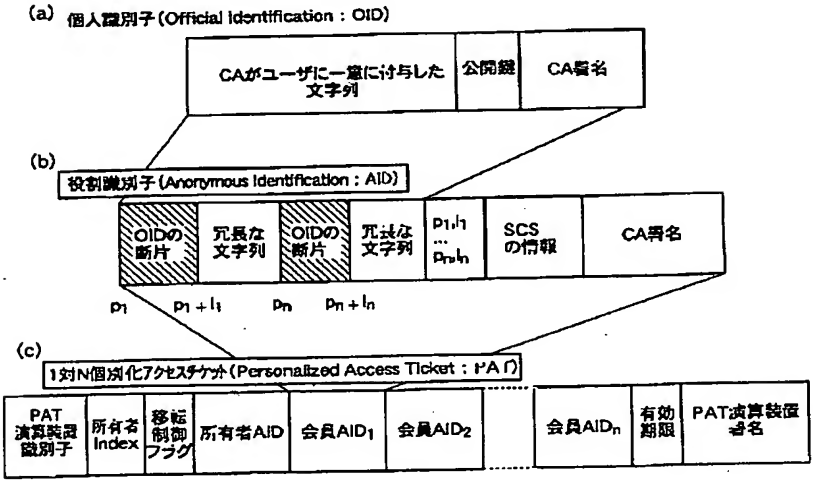
【図7】



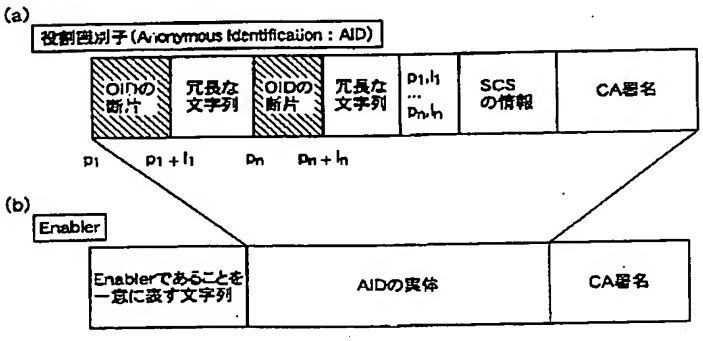
【図10】



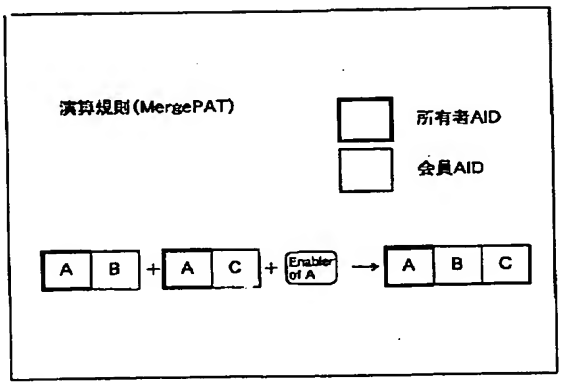
【図8】



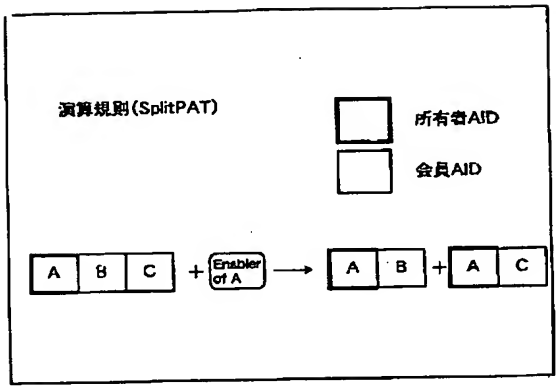
【図9】



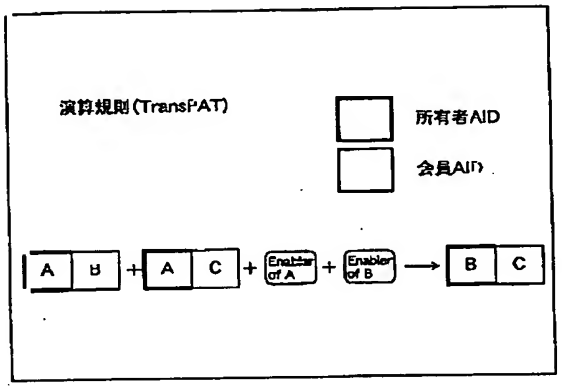
【図11】



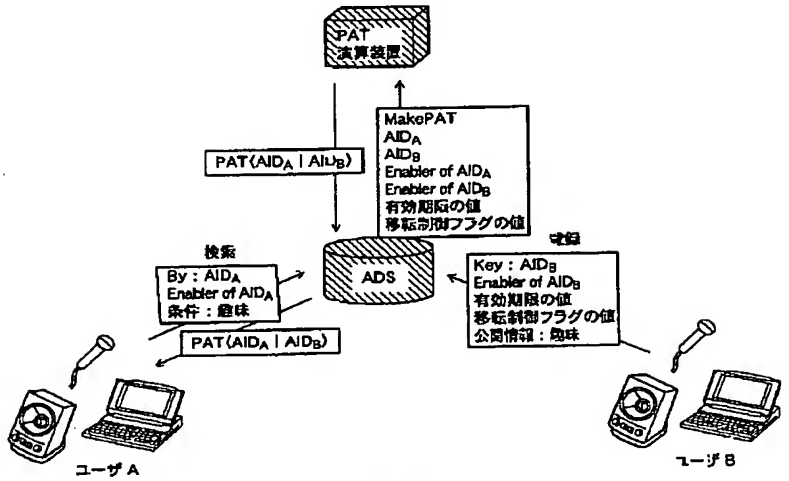
【図１２】



【図１３】

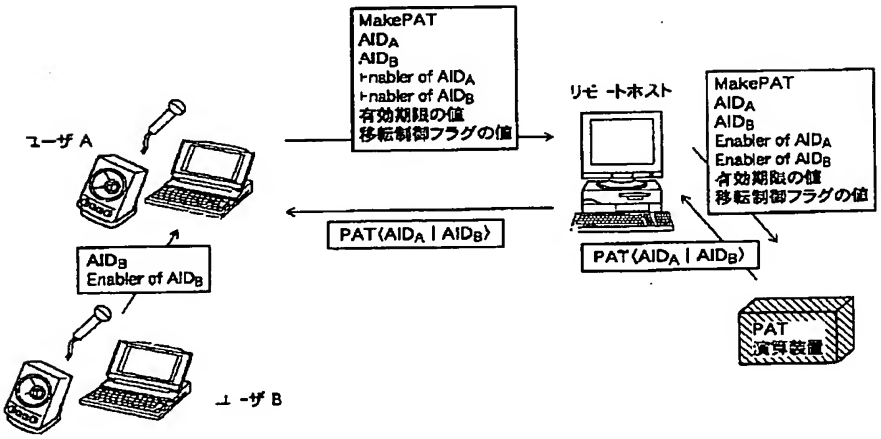


【図１４】



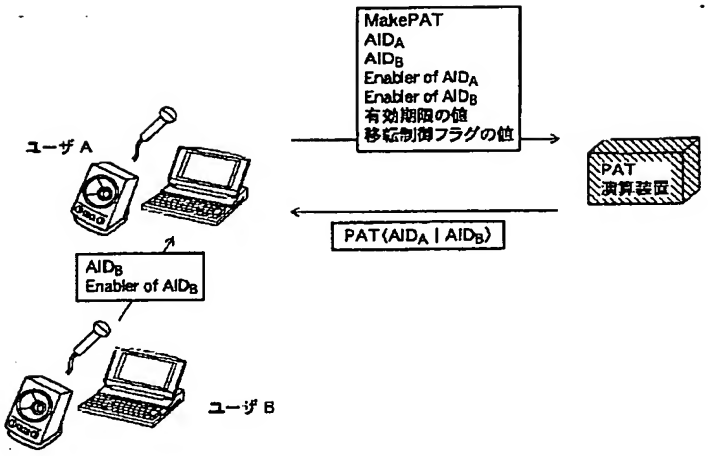
システム構成(1)

【図１６】



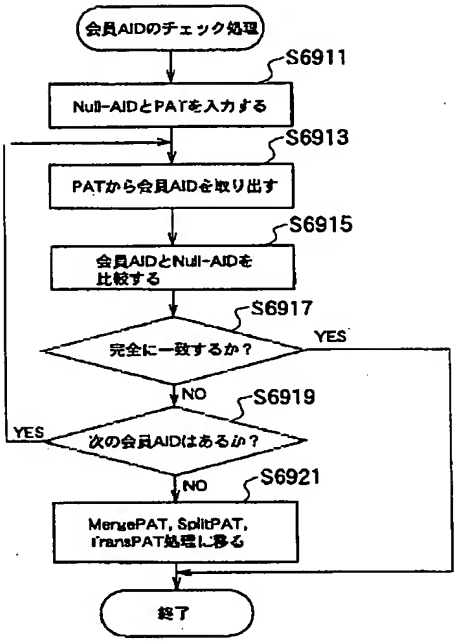
システム構成(3)

【図15】

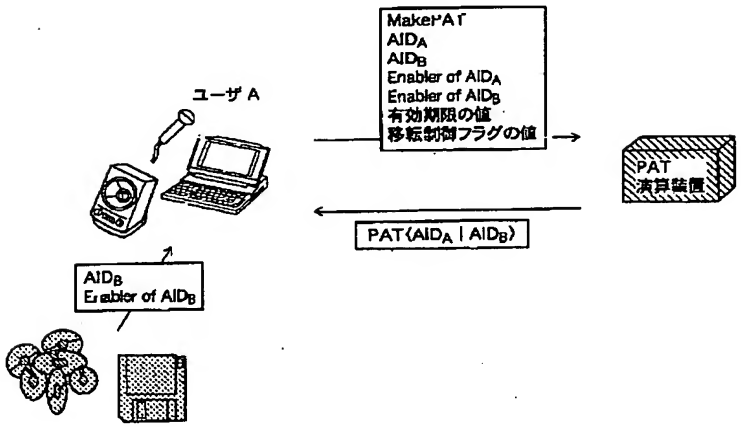


システム構成(2)

【図32】

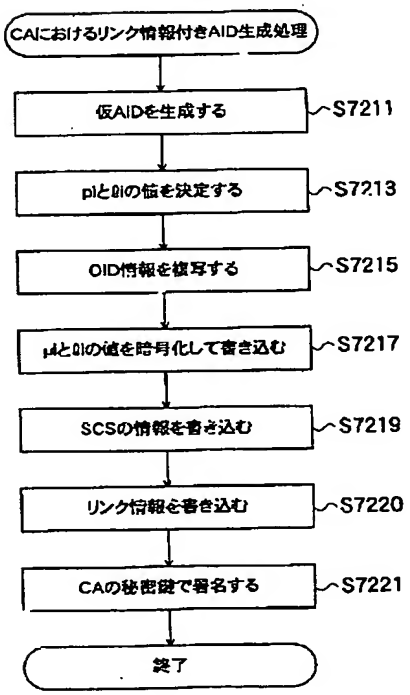


【図17】



システム構成(4)

【図35】

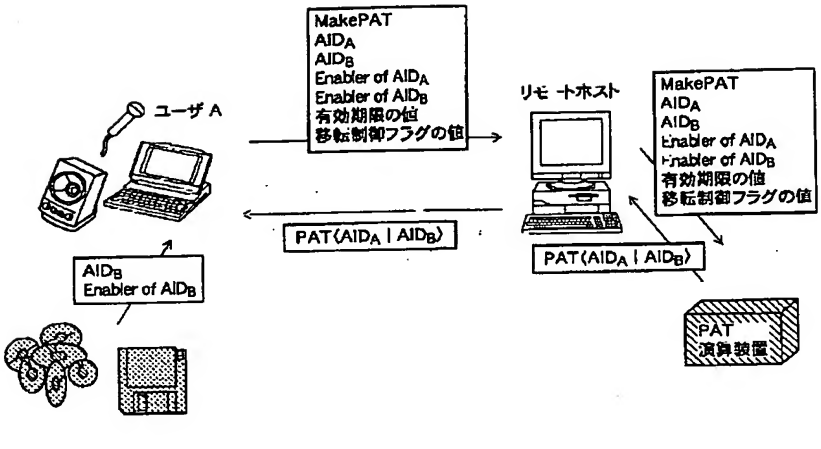


【図26】

Enabler of Null-AIDのデータ構造

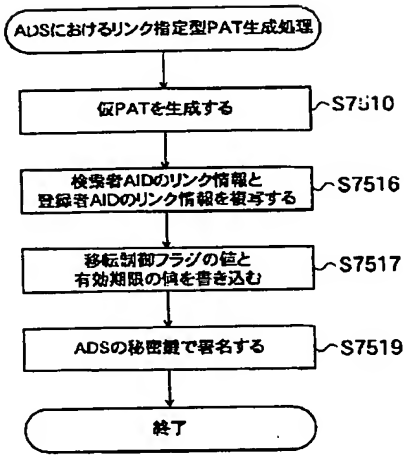
Enablerであることを一意に表す文字列	Null-AIDの実体	CA署名

【図18】

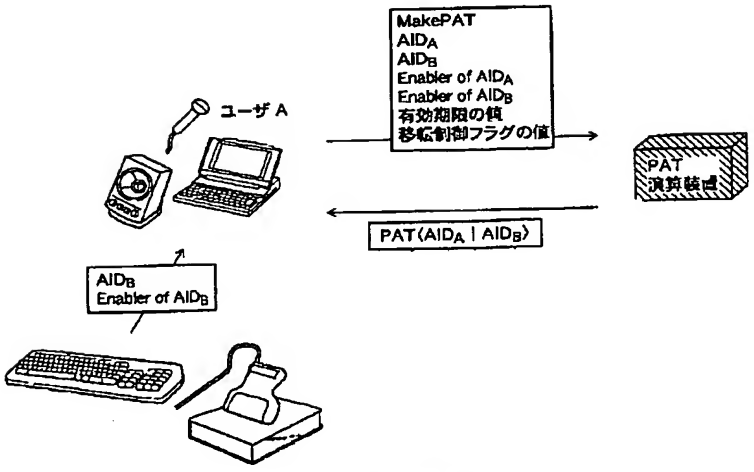


システム構成(5)

【図36】

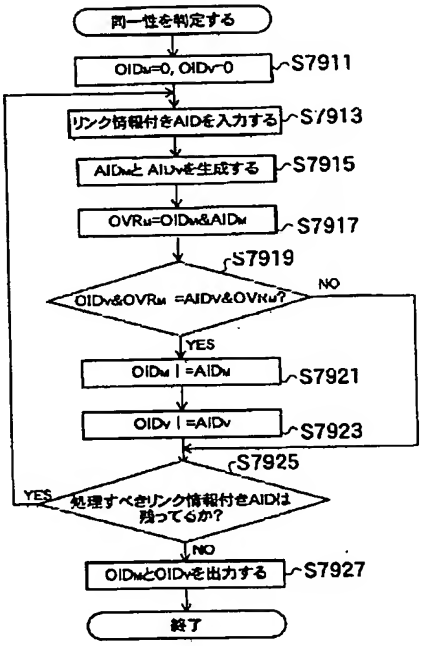


【図19】



システム構成(6)

【図38】

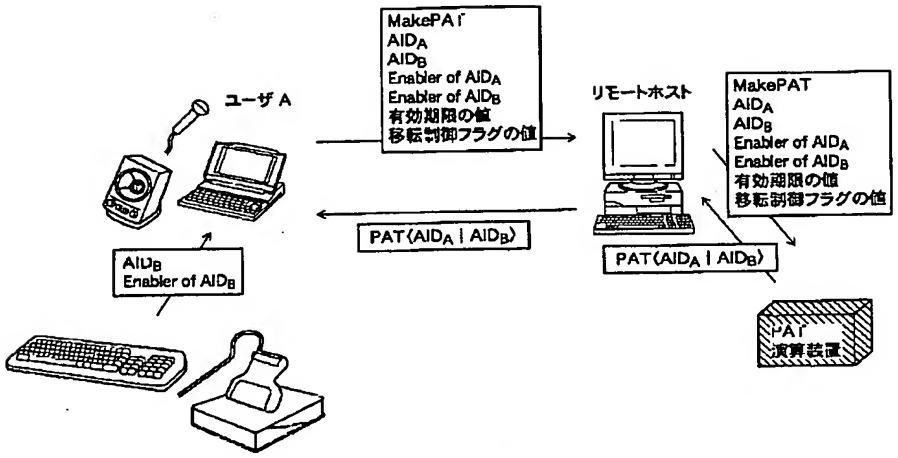


【図29】

God-AIDのデータ構造

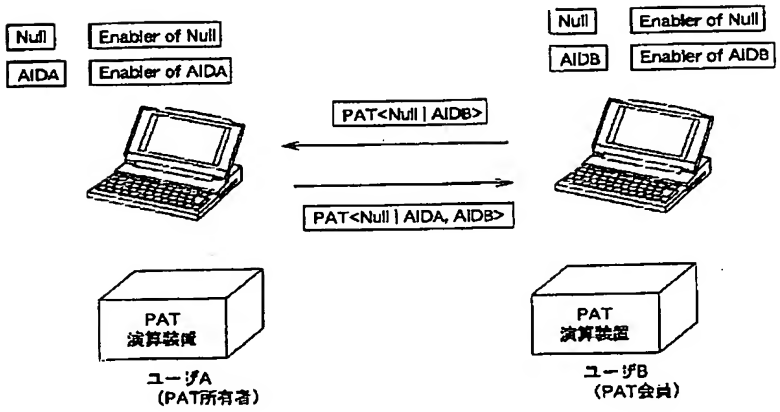
God-AIDであることを一意に表す文字列	CA署名

【図20】

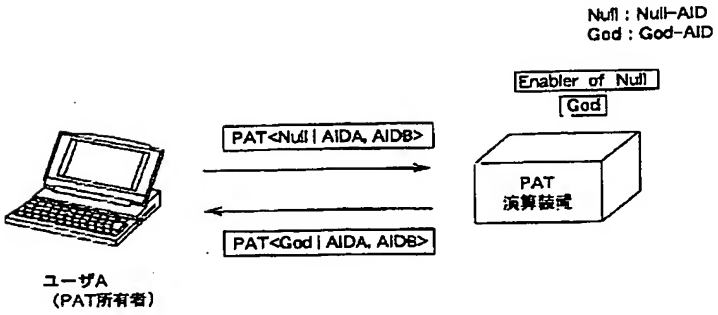


システム構成(7)

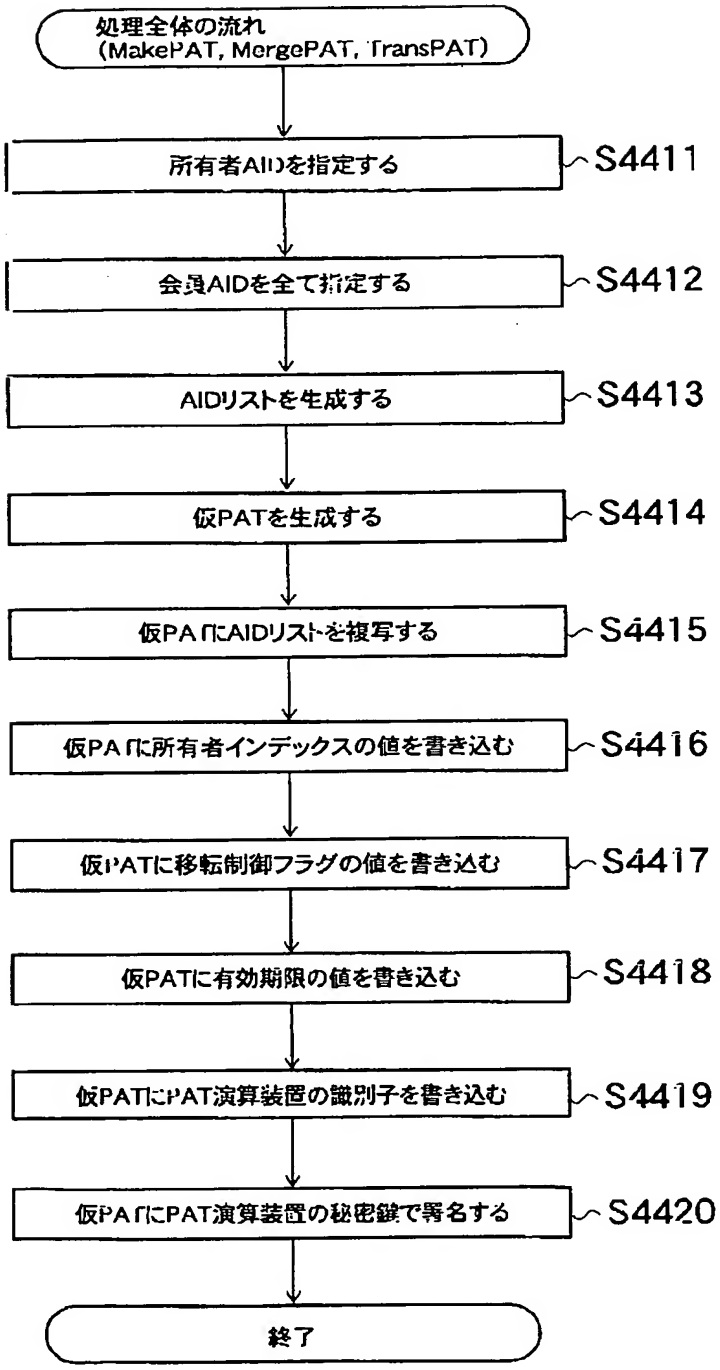
【図27】



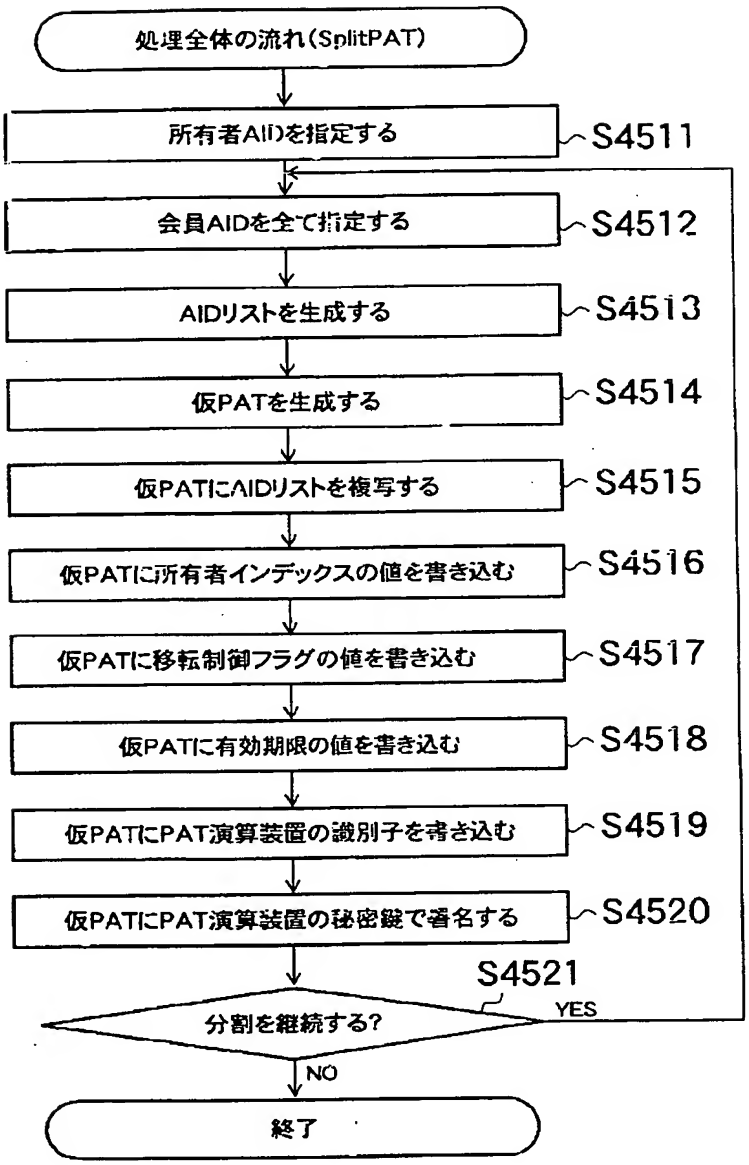
【図30】



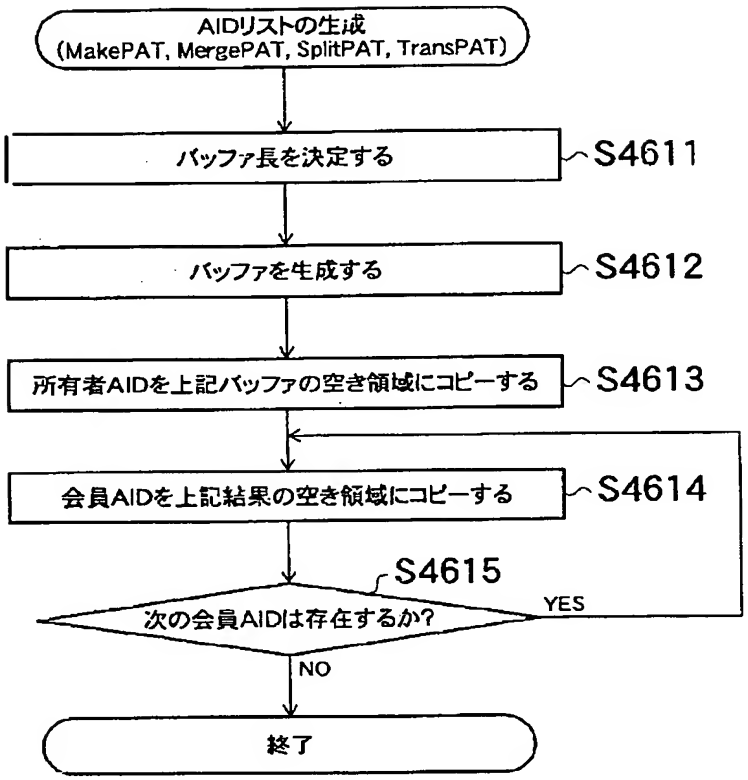
【図21】


処理全体の流れ
(MakePAT, MergePAT, TransPAT)
所有者AIDを指定する
S4411
会員AIDを全て指定する
S4412
AIDリストを生成する
S4413
仮PATを生成する
S4414
仮PATにAIDリストを複写する
S4415
仮PATに所有者インデックスの値を書き込む
S4416
仮PATに移転制御フラグの値を書き込む
S4417
仮PATに有効期限の値を書き込む
S4418
仮PATにPAT演算装置の識別子を書き込む
S4419
仮PATにPAT演算装置の秘密鍵で署名する
S4420
終了

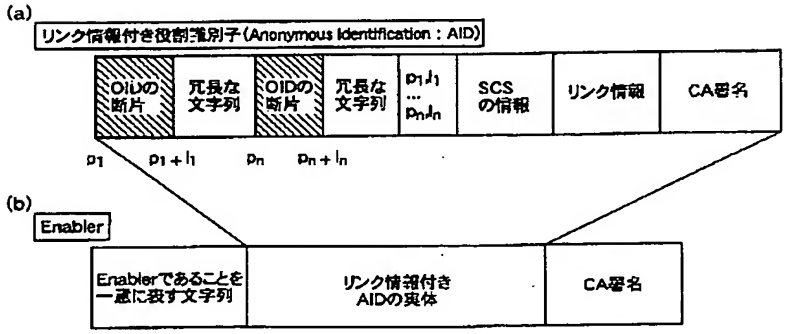
【図22】


処理全体の流れ(SplitPAT)
所有者AID)を指定する
S4511
会員AIDを全て指定する
S4512
AIDリストを生成する
S4513
仮PATを生成する
S4514
仮PATにAIDリストを複写する
S4515
仮PATに所有者インデックスの値を書き込む
S4516
仮PATに移転制御フラグの値を書き込む
S4517
仮PATに有効期限の値を書き込む
S4518
仮PATにPAT演算装置の識別子を書き込む
S4519
仮PATにPAT演算装置の秘密鍵で署名する
S4520
S4521
分割を継続する?
YES
NO
終了

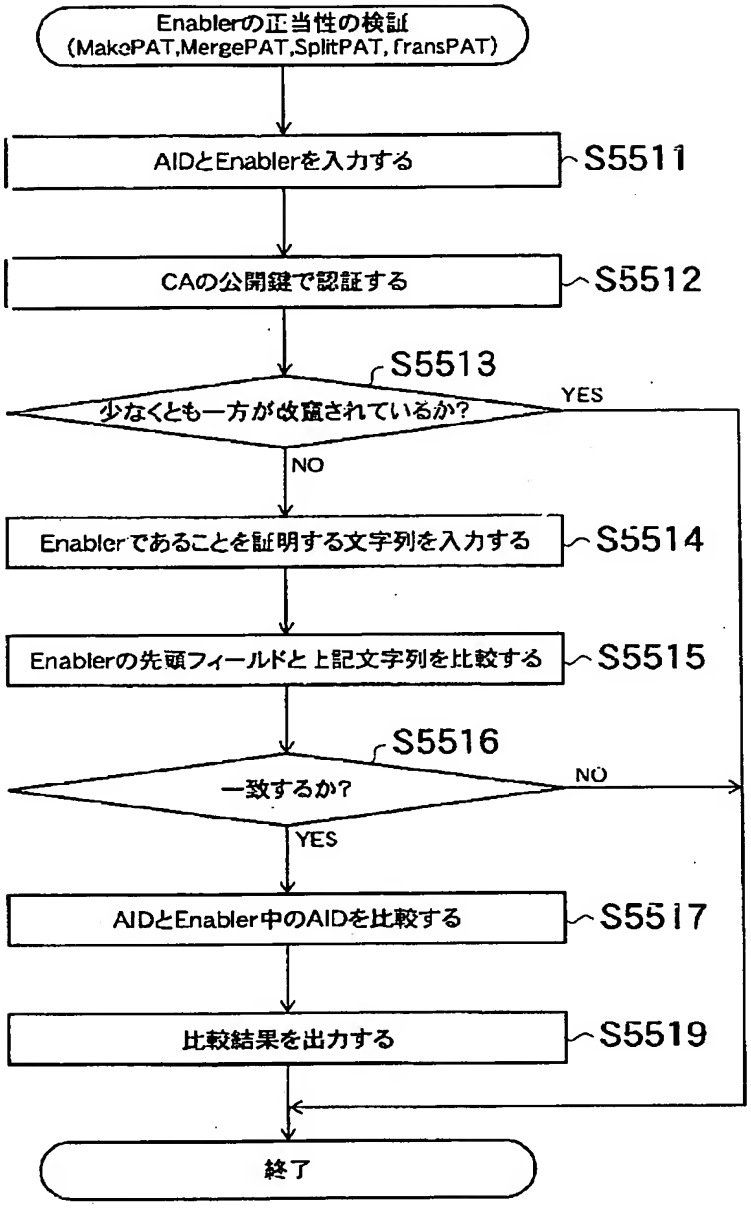
【図２３】


AIDリストの生成
(MakePAT, MergePAT, SplitPAT, TransPAT)
バッファ長を決定する
S4611
バッファを生成する
S4612
所有者AIDを上記バッファの空き領域にコピーする
S4613
会員AIDを上記結果の空き領域にコピーする
S4614
S4615
次の会員AIDは存在するか?
YES
NO
終了

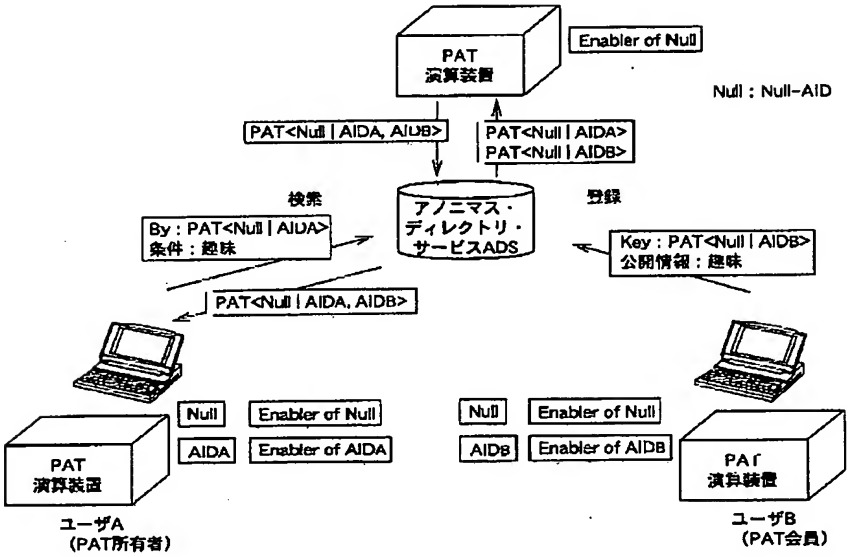
【図４１】


(a)
リンク情報付き役割識別子(Anonymous Identification : AID)
OIDの断片
冗長な文字列
OIDの断片
冗長な文字列
SCSの情報
リンク情報
CA署名
(b)
Enabler
Enablerであることを一意に表す文字列
リンク情報付きAIDの実体
CA署名

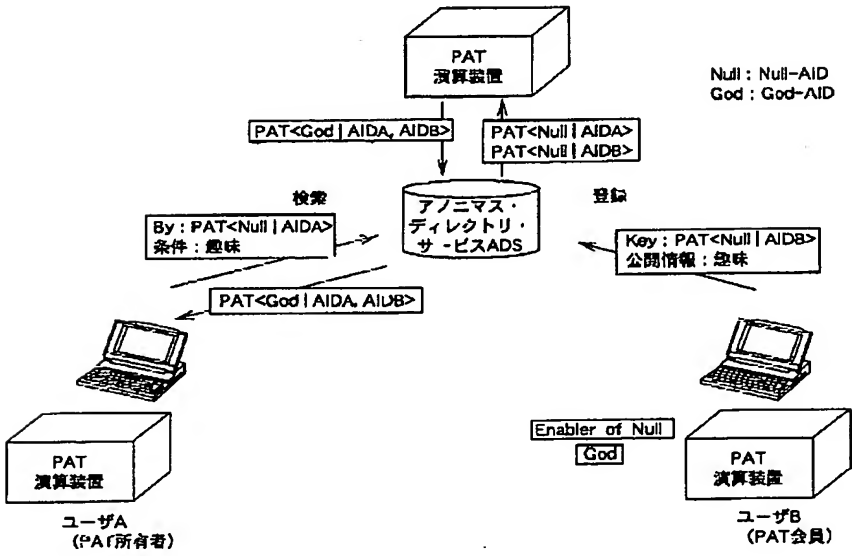
【図24】


Enablerの正当性の検証
(MakePAT,MergePAT,SplitPAT,TransPAT)
AIDとEnablerを入力する
S5511
CAの公開鍵で認証する
S5512
S5513
少なくとも一方が改竄されているか?
YES
NO
Enablerであることを証明する文字列を入力する
S5514
Enablerの先頭フィールドと上記文字列を比較する
S5515
S5516
一致するか?
NO
YES
AIDとEnabler中のAIDを比較する
S5517
比較結果を出力する
S5519
終了

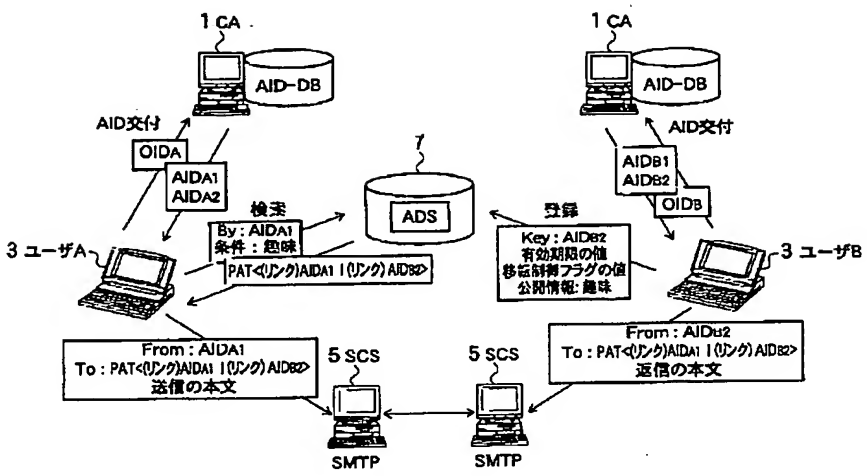
【図28】


PAT
演算装置
Enabler of Null
Null : Null-AID
PAT<Null | AIDA, AIDB>
PAT<Null | AIDA>
PAT<Null | AIDB>
検索
登録
By : PAT<Null | AIDA>
条件 : 趣味
アノニマス・
ディレクトリ・
サービスADS
Key : PAT<Null | AIDB>
公開情報 : 趣味
PAT<Null | AIDA, AIDB>
Null
Enabler of Null
AIDA
Enabler of AIDA
Null
Enabler of Null
AIDB
Enabler of AIDB
PAT
演算装置
PAT
演算装置
ユーザA
(PAT所有者)
ユーザB
(PAT会員)

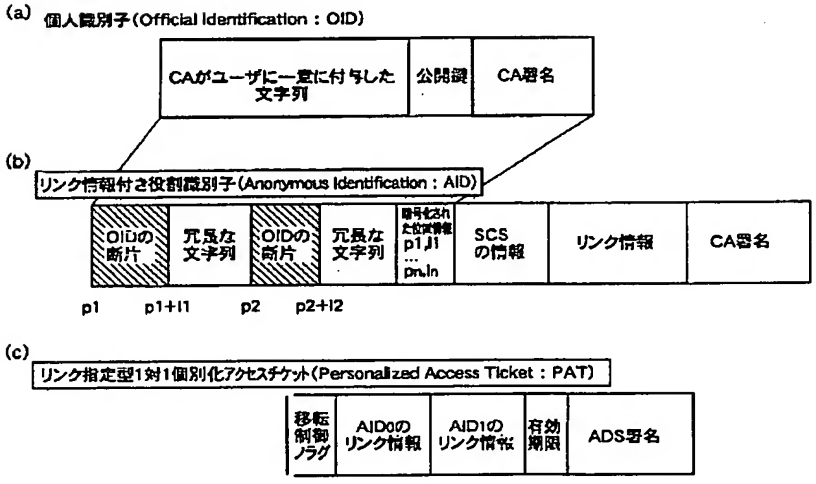
【図31】


PAT
演算装置
Null : Null-AID
God : God-AID
PAT<God | AIDA, AIDB>
PAT<Null | AIDA>
PAT<Null | AIDB>
検索
登録
By : PAT<Null | AIDA>
条件 : 趣味
アノニマス・
ディレクトリ・
サービスADS
Key : PAT<Null | AIDB>
公開情報 : 趣味
PAT<God | AIDA, AIDB>
Enabler of Null
God
PAT
演算装置
PAT
演算装置
ユーザA
(PAT所有者)
ユーザB
(PAT会員)

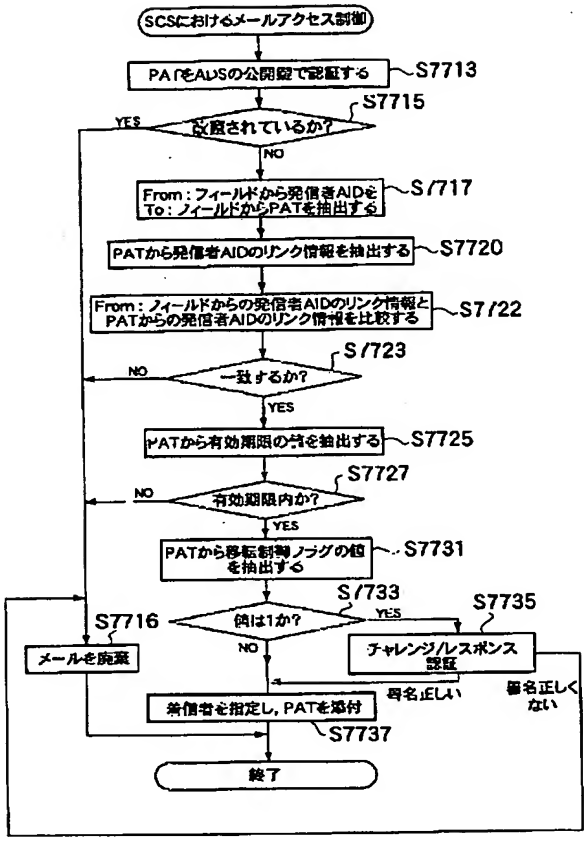
【図33】


1 CA
AID-DB
AID交付
OIDA
AIDA1
AIDA2
検索
By : AIDA1
条件：趣味
PAT<リンク)AIDA1 I(リンク) AIDB2>
ADS
登録
Key : AIDB2
有効期限の値
移転制御フラグの値
公開情報: 趣味
1 CA
AID-DB
AID交付
AIDB1
AIDB2
OIDB
3 ユーザA
3 ユーザB
From : AIDA1
To : PAT<リンク)AIDA1 I(リンク) AIDB2>
送信の本文
5 SCS
5 SCS
From : AIDB2
To : PAT<リンク)AIDA1 I(リンク) AIDB2>
返信の本文
SMTP
SMTP

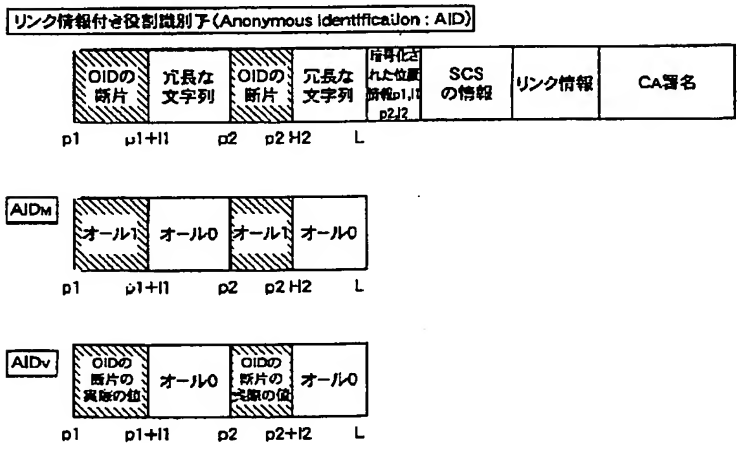
【図34】


(a) 個人識別子(Official Identification : OID)
CAがユーザに一意に付与した文字列
公開鍵
CA署名
(b)
リンク情報付き役割識別子(Anonymous Identification : AID)
OIDの断片
冗長な文字列
OIDの断片
冗長な文字列
暗号化された位置情報 p1,I1 ... pn,In
SCSの情報
リンク情報
CA署名
p1
p1+l1
p2
p2+l2
(c)
リンク指定型1対1個別化アクセスチケット(Personalized Access Ticket : PAT)
移転制御フラグ
AID0のリンク情報
AID1のリンク情報
有効期限
ADS署名

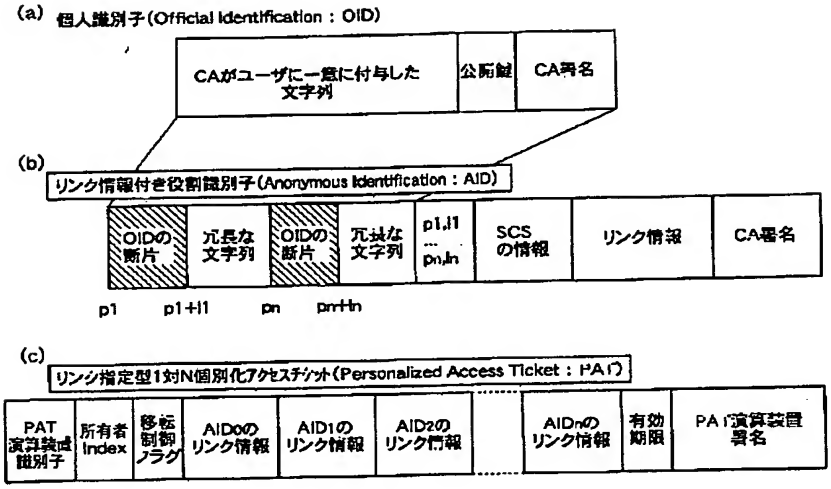
【図37】


SCSにおけるメールアクセス制御
PATをAUSの公開鍵で認証する
S7713
改竄されているか?
S7715
YES
NO
From:フィールドから発信者AIDを
To:フィールドからPATを抽出する
S7717
PATから発信者AIDのリンク情報を抽出する
S7720
From:フィールドからの発信者AIDのリンク情報と
PATからの発信者AIDのリンク情報を比較する
S7722
一致するか?
S7723
NO
YES
PATから有効期限の情を抽出する
S7725
有効期限内か?
S7727
NO
YES
PATから移転制御フラグの値
を抽出する
S7731
値は1か?
S7733
YES
NO
S7735
S7716
メールを廃棄
チャレンジ/レスポンス
認証
署名正しい
署名正しく
ない
発信者を指定し, PATを添付
S7737
終了

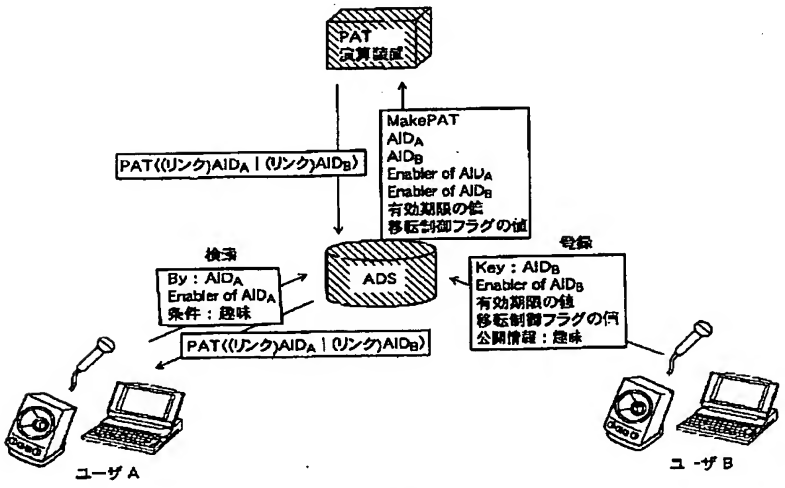
【図39】


リンク情報付き役割識別子(Anonymous Identification : AID)
OIDの断片
冗長な文字列
OIDの断片
冗長な文字列
暗号化された位置情報p1,l1 p2,l2
SCSの情報
リンク情報
CA署名
p1
p1+l1
p2
p2 H2
L
AIDM
オール1
オール0
オール1
オール0
AIDV
OIDの断片の真値の位
オール0
OIDの断片の元数の位
オール0

【図４０】

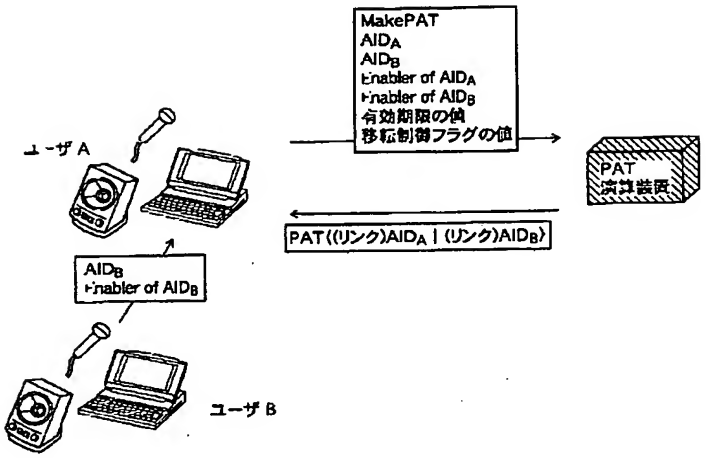


【図４２】



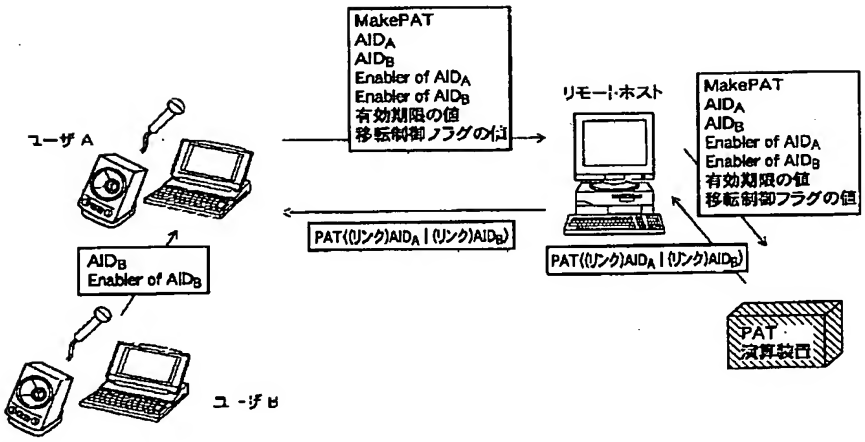
システム構成(1)

【図43】



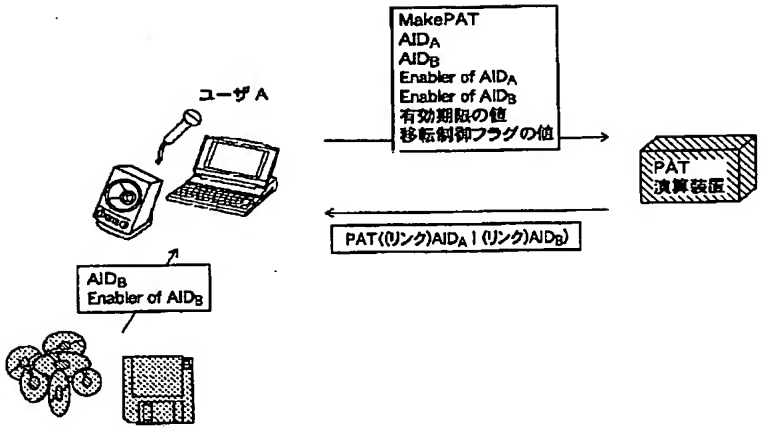
システム構成(2)

【図44】



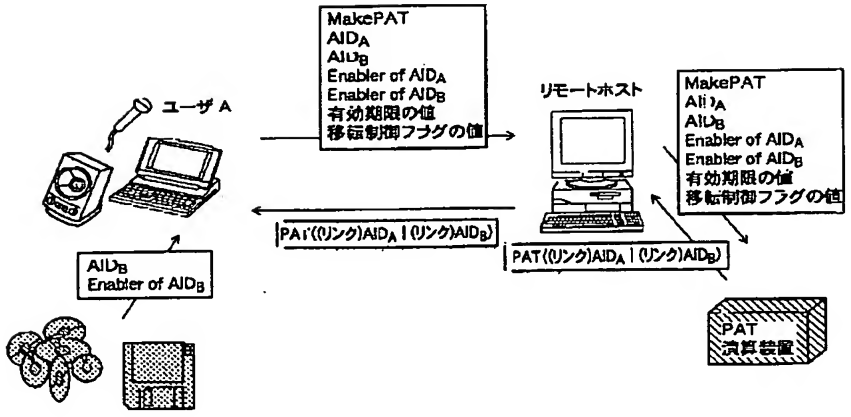
システム構成(3)

【図45】



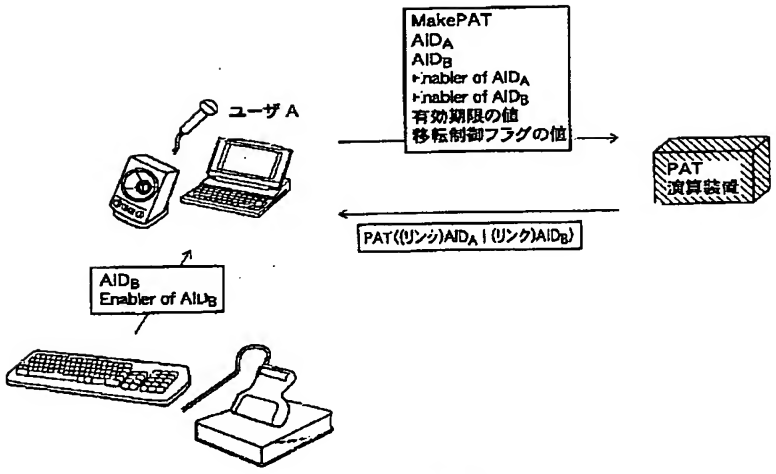
システム構成(4)

【図46】



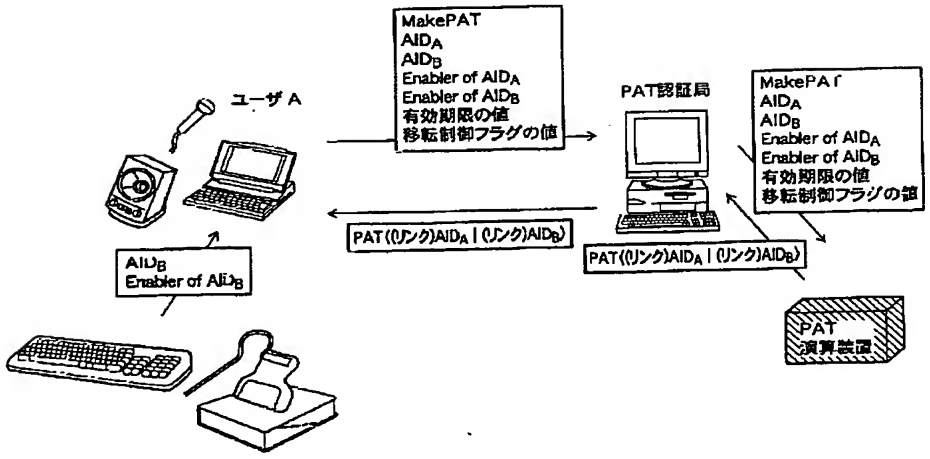
システム構成(5)

【図４７】



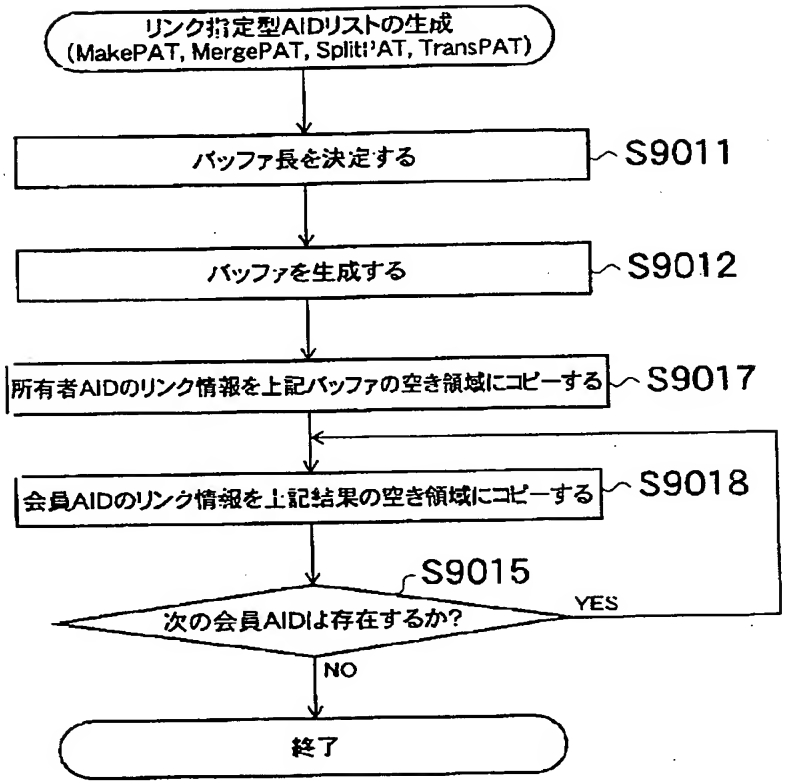
システム構成(6)

【図４８】



システム構成(7)

【図49】



フロントページの続き

(31)優先権主張番号　特願平10−315172
(32)優先日　平成10年11月5日(1998．11．5)
(33)優先権主張国　日本（ＪＰ）
(72)発明者　市川　晴久
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム(参考)　5B089 GA01 JB22 KA17 KB11 KB13 KC51 KC58
5J104 AA07 AA09 KA01 KA05 MA01 NA02 NA36 NA38 PA08
5K030 GA15 HA06 KA04 LD19 LD20
9A001 BB04 CC03 DD10 FF03 JJ14 KK56 LL03 LL09